Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Metody zajištění redundance v počítačových sítích

Methods of Ensuring Redundancy in Computer Networks

2018 **Bc. Jiří Pijáček**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Jiří Pijáček**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Metody zajištění redundance v počítačových sítích
Methods of Ensuring Redundancy in Computer Networks

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování různých způsobů zajištění redundance v počítačových sítích v laboratorním prostředí s využitím přepínačů a směrovačů Cisco a Huawei.

Osnova práce:
1. Popište různé způsoby zajištění redundance v počítačových sítích.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři způsoby zajištění redundance v počítačových sítích z hlediska síťových zařízení a přenosových cest. Použijte k tomu přepínače a směrovače Cisco a Huawei. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu přepínačů a směrovačů Cisco a Huawei v těchto sítích.
4. Srovnejte jednotlivá řešení. Zhodnoťte výhody a nevýhody jejich použití.

Seznam doporučené odborné literatury:

[1] TEARE, Diane, et al. *CCNP Routing and Switching Foundation Learning Library: Foundation Learning for CCNP ROUTE, SWITCH, and TSHOOT (642-902, 642-813, 642-832).* 1st ed. Indianapolis: Cisco Press, 2010. ISBN-13: 978-1-58705-885-1.
[2] Dokumentace k zařízením Huawei a Cisco.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2016
Datum odevzdání: 30.04.2018

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky 1D16 OSTRAVA

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *30. dubna 2018*

podpis studenta

Poděkování

Rád bych poděkoval Ing. Petrovi Machníkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Abstrakt

Diplomová práce se zabývá problematikou redundantního zapojení síťových prvků dvou výrobců Cisco a Huawei. Práce se zabývá popsáním různých technik na linkové a síťové vrstvě. V práci jsou zmíněny otevřené průmyslové standardy i proprietární technologie, které budou navzájem porovnány. Praktická část se věnuje zapojení a ověření kompatibility v laboratorních podmínkách. Bude také provedeno zapojení dvou proprietárních technik, které budou navzájem spolupracovat. Práce by měla sloužit jako ucelený studijní materiál pro redundantní zapojení různých výrobců Cisco a Huawei.

Klíčová slova

LAN; agregace linek; NIC-teaming; Etherchannel; Bonding; LACP; VRRP; HSRP; STP; RSTP; MSTP; PVST; round-robin; hash; XOR; Bit; M-LAG; Smartlink; NAT; dual-home; RRPP; Multicast; Broadcast

Abstract

This diploma thesis deals with the redundant connection of two network elements manufacturers Cisco and Huawei. The thesis deals with the description of different techniques on the data link layer and network layer. In the work are mentioned open industry standards and proprietary technologies that will be compared to each other. The practical part deals with integration and verification of compatibility in laboratory conditions. It will also involve the involvement of two proprietary techniques that will work together. The work should serve as a comprehensive study material for the redundant involvement of various Cisco and Huawei manufacturers.

Key words

LAN; aggregation; NIC-teaming; Etherchannel; Bonding; LACP; VRRP; HSRP; STP; MSTP; RSTP; PVST; round-robin; hash; XOR; Bit; M-LAG; Smartlink; NAT; dual-home; RRPP; Multicast; Broadcast

Seznam použitých symbolů

Symbol	Jednotky	Význam symbolu
Mbit	Mbit/s	Přenosová rychlost v mega bitech
Gbit	Gbit/s	Přenosová rychlost v giga bitech

Seznam použitých zkratek

Zkratka	Význam
Bin	Binární jednotka
CLI	Command Line Interface
Dst-IP	Destination-Internet Protocol
Dst-MAC	Destination-Media Access Control
FHRP	First Hop Redundancy Protocol
GLBP	Gateway Load Balaning Protocol
HSRP	Hot Standby Routing Protocol
IRF	Inteligent Resilient Framework
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Media Access Control
Mbit/s	Mega Bit per second
M-LAG	Multi-Chassis Link Aggregation Group
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NIC-teaming	Network interface card - teaming
PVST	Per Vlan Spanning Tree Protocol
QoS	Quality of Service
RRPP	Rapid Ring Protection Protocol
RSTP	Rapid Spanning Tree Protocol
STP	Spanning Tree Protocol
Src-IP	Source-Internet Protocol
Src-MAC	Source-Media Access Protocol
VLAN	Virtual Local Area Network
VSS	Virtual Switching System
VoIP	Voice over Internet Protocol
VRRP	Virtual Router Redundancy Protocol

XOR	exkluzivní OR

Obsah

Úvod

Počítačové sítě potkáváme takřka všude, v zaměstnání, ve škole, při cestování. Člověk je používá neustále, někdy i nevědomě. Pro nepřetržitý provoz sítí, nebo internetu je potřeba zajistit jejich chod pomocí různých technik. Existuje mnoho nástrojů zajišťující vysokou dostupnost, ať už jsou to virtualizační nástroje, které dokáží během okamžiku migrovat virtuální stroj na jiné fyzické zázemí, nebo směrovací protokoly, které při zjištění nedostupnosti sítě vypočítají cestu k cíli jinudy. Dalo by se pokračovat ve výpisu mnoha dalších technologií, ale tato práce si klade za cíl zabezpečit vysokou dostupnost pomocí redundantního spojení mezi prvky různých výrobců.

Pojem redundance má jiný význam ve světě, než v počítačových sítích. Redundancí rozumíme nadměrné, zbytečné opakování, mnohomluvnost, atd. V počítačových sítích nabývá významu opatření proti poruše systému sítě prostřednictvím zavedení dalších, nebo duplicitních systémů, zařízení, prvků, nebo linek. Redundance s sebou přináší určitý druh vysoké dostupnosti. V některých případech redundantní zapojení nabízí vyvažování zátěže a větší přenosovou rychlost. Většina poskytovatelů internetového připojení, nebo firem starající se o síťovou infrastrukturu vychází z toho, že je dobré mít síť tvořenou prvky jednoho výrobce.

Záleží, z jakého úhlu pohledu se na věc podíváme. Pokud zvolíme cestu nákupu aktivních prvků jednoho výrobce, získáme tím přístup k proprietárním technologiím. Prvky jednoho typu, můžeme snadněji hromadně konfigurovat, nebo aktualizovat. Naopak to bude mít negativní dopad ve smyslu uzavřenosti sítě. Nebo se můžeme vydat cestou standardů, jejichž hlavní výhodou je otevřenost a flexibilita. Práce si klade za cíl zapojení aktivních prvků různých výrobců v redundantním zapojení. Je to z důvodu, že může nastat situace, kdy budeme muset provést redundantní spojení a po ruce nemáme stejné prvky od jednoho výrobce.

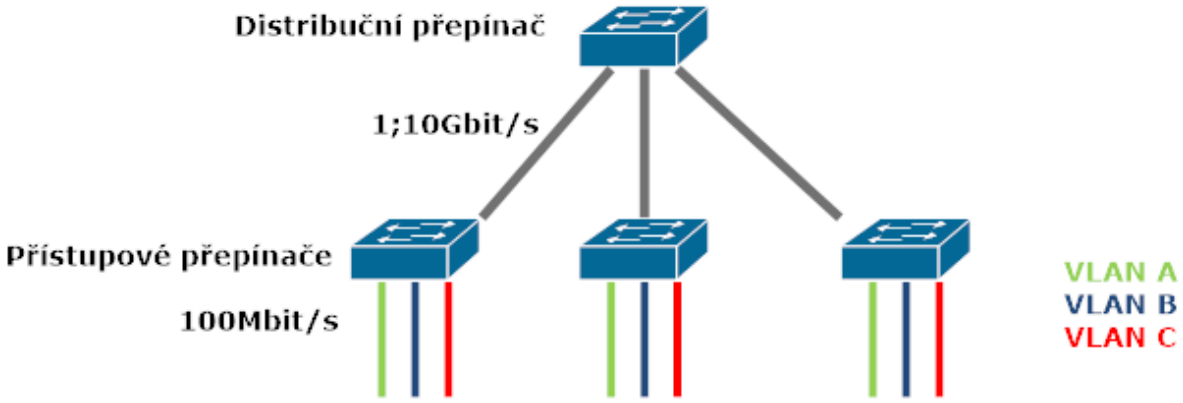
Teoretická část práce se rozděluje do dvou bloků, v prvním se věnuji možnostem redundance na linkové vrstvě, popíšu spojení několika fyzických portů do jednoho logického. Popíšu vyjednávací protokoly, které vytvářejí logickou linku automaticky. Popíšu různé druhy vyvažování zátěže, protože bez správně nastavené metody vyvažování bychom nezískali maximální potenciál logického kanálu. Bude probráno proprietární řešení redundantního spojení od výrobce Huawei, poté řešení od Cisco. Nakonec budou tyto techniky zkombinovány tak, aby navzájem mohli spolupracovat. V praktické části se zaměřím na zapojení Etherchannel, kde budu provádět ověření teoretických poznatků v laboratorním prostředí. Poté provedu zapojení dvou proprietárních technik, které budou spolupracovat. Nakonec provedu zapojení redundantních výchozích bran a ověřím kompatibilitu mezi prvky různých výrobců.

1 Agregace Linek

Agregace linek je termín, který vystihuje metody spojení (agregace) síťových linek. Různí výrobci volí různé termíny, můžeme se setkat například s pojmy Etherchannel (Cisco), Bonding (Linux), Eth-trunk (Huawei), NIC-teaming (windows). V rámci práce budu používat jednotně termín Etherchannel.

V sítích, kde jsou zdroje, nebo servery umístěné daleko od uživatele kde je potřebuje, můžou některé linky mezi přepínači a směrovači být vytíženy. V komunikacích typu všichni se všema, jako jsou videa, interaktivní chat, hlas přes IP (VoIP), navyšují potřebu přenosové rychlosti mezi cílem a zdrojem v síti LAN. Ve stejnou chvíli však potřebují časově kritické aplikace taky určitou pevnou přenosovou rychlost. A zde nastává problém, uživatelé chtějí buď snížit agregaci (ve smyslu sdílení linky), nebo navýšit rychlost linek.

Rychlost těchto linek může být navýšena, ale jen do určitého bodu. Agregace linek, neboli Etherchannel je technologie, která umožňuje zvětšení propustnosti a zajištění větší spolehlivosti vytvořením logické linky složené z několika fyzických linek resp. portů.



Obrázek 1.1: *Agregace linek*

Provoz jdoucí z několika VLAN na 100Mbit/s linkách na přístupových přepínačích se potřebuje dostat na distribuční přepínače propojující LAN s okolním světem, obrázek č. 1.1. Obvykle bývá přenosová rychlost mezi přepínači větší než 100Mbit/s aby pokryla zátěž jdoucí ze všech VLAN. Prvním řešením jak zvýšit propustnost je použití rychlejších portů jako jsou 1Gbit/s nebo 10Gbit/s. Jakmile ale rychlost narůstá na jednotlivých VLAN, tak se může tohle řešení zdát limitující, protože nejrychlejší port nedokáže pokrýt veškerou zátěž. Druhé řešení by bylo propojit jednotlivé přepínače mezi sebou více porty pro zvýšení celkové rychlosti, ale zde by se

projevovaly smyčky, které by musel STP odstranit pomocí blokování portů, takže výsledek by byl nulový. Ani použití QoS technologie v mnoha případech nebude mít význam, protože tímto jen zamezíme, nebo upřednostníme určitý provoz, ale ve výsledku větší propustnosti nedocílíme. Technologie Etherchannel byla vytvořena původně společností Kalpana kterou později odkoupila společnost CISCO. V roce 2000 prošel Etherchannel standardizací pod označením IEEE 802.3ad.

1.1 Výhody agregace linek

- Staví na existujících portech. Není potřeba vylepšovat, nebo zakupovat rychlejší rozhraní mezi přepínači k získání rychlejšího a dražšího připojení.

- Veškeré konfigurace můžou být provedeny na Etherchannel rozhraní namísto každého portu individuálně. To zajišťuje konfigurační konzistenci napříč několika porty.

- Je možné použít vyvažování zátěže mezi linkami, které tvoří část stejného Etherchannel. Záleží na hardwarové platformě, můžeme implementovat několik metod napříč fyzickými linkami. Etherchannel zajišťuje vysokou dostupnost. Pokud jeden, nebo více portů v zapojení Etherchannel vypadne, tak ostatní porty si převezmou jeho práci. [1]

1.2 Vyvažovací metody Etherchannel

Aby mohl přepínač, nebo směrovač co nejefektivněji využívat možnosti Etherchannel zapojení, je dobré si vysvětlit základní principy. Při sestavování portů do Etherchannel je již nastavena metoda vyvažování zátěže, každý výrobce ji volí podle sebe. A ne každý výrobce nabízí všechny metody. Druhy vyvažování jsou následující:

- dst-ip: Pakety jdoucí do Etherchannel jsou distribuovány na základě cílových IP adresách příchozích paketů. Proto k zajištění vyvažování jsou pakety jdoucí z jedné IP adresy na několik cílových IP adres poslány různými porty. Ale pakety jdoucí z různých IP adres na jednu cílovou budou vždy poslány jedním portem.

- dst-mac: Pakety jdoucí do Etherchannel jsou distribuovány na základě cílové MAC adrese příchozího paketu. Proto pakety se stejnou cílovou MAC adresou jsou

poslány stejným portem, ale pakety s různou cílovou MAC adresou jsou poslány různými porty.

- src-dst-ip: Pakety jdoucí do Etherchannel jsou distribuovány na základě zdrojové a cílové IP adrese příchozího paketu. Proto k zajištění vyvažování pakety jdoucí z různých IP adres na různé, nebo stejnou cílovou IP adresu budou distribuovány různými porty. Tato metoda je kombinací src-ip a dst-ip a může být použita, když si nejsme jisti, jestli použít src-ip nebo dst-ip na patřičném přepínači.

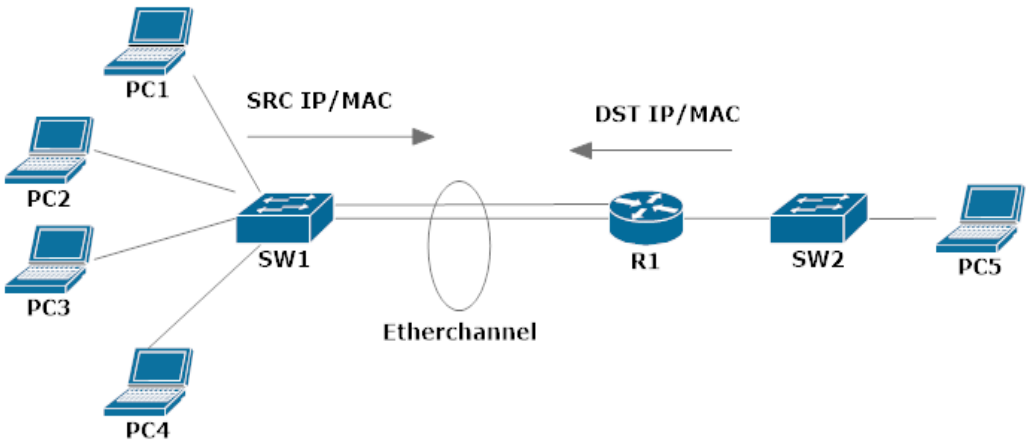
- src-ip: Pakety jdoucí do Etherchannel jsou distribuovány napříč porty na základě zdrojové IP adresy příchozího paketu.

- src-port: Zátěž je distribuována na základě zdrojového portu obsaženého v L4 hlavičce. Proto k zajištění vyvažování zátěže různými porty musíme volit různé zdrojové L4 porty. Zde nezáleží, jestli pakety směřují na různé MAC adresy nebo IP adresy, musí mít různé zdrojové porty. Tuto možnost nabízejí CISCO přepínače vyšších řad.

- dst-port: Používá cílové číslo portu transportní vrstvy k vypočítání odchozího portu jako u předchozí metody vyvažování.

- src-dst-port: Zátěž je distribuovaná na základě zdrojového a cílovou portu transportní vrstvy. Používá se, pokud není jisté, jestli požít src-port nebo dst-port metodu.[2]

Různé vyvažovací metody mají různé výhody, volba konkrétní metody by měla být založena na pozici přepínače, nebo směrovače v síti a na druhu provozu, který bude vyvažován. Na obrázku č. 1.2 jsou vlevo čtyři klientské stanice komunikující s klientskou stanicí PC5. Protože má směrovač jednu MAC adresu, tak bude na přepínači použita src metoda přeposílání, ta zajišťuje, že přepínač bude využívat veškerou šířku pásma směrem ke směrovači, protože bude vyvažovat na základě zdrojových informací, ať už MAC adresy, nebo IP adresy. Směrovač bude mít nastavenu dst metodu, protože velké množství klientských stanic zajišťuje velké množství IP a MAC adres, takže provoz bude rovnoměrně distribuován ze směrovače na základě těchto hodnot. Pokud bychom zvolili na přepínači dst MAC metodu, tak provoz z přepínače na směrovač půjde vždy jedním portem. Pokud bychom zvolili src MAC metodu na směrovači, tak provoz poteče vždy jedním portem, protože MAC adresa bude vždy stejná.



Obrázek 1.2: *Etherchannel metody*

Pokud jsou za přepínači tvořící Etherchannel obrázek č.1.2 pouze směrovače, tak vyvažování zátěže na základě MAC adres nemá smysl, protože MAC adresy budou vždy stejné. Kdyby směrovače prováděli NAT, tak nemá smysl použít jakoukoliv metodu vyvažování zátěže z linkové nebo síťové vrstvy, protože MAC adresy a stejně tak i IP adresy budou pokaždé stejné. Museli bychom zvolit metodu vyvažování zátěže na základě portů transportní vrstvy.

Obrázek 1.3: *Etherchannel se směrovači*

1.3 Datové toky

Následující výpočty a metody platí pouze pro přepínače a směrovače značky Cisco. Pomocí určení metody vyvažování se přepínač podívá do L2, L3, nebo L4 hlavičky, záleží, jakou vyvažovací metodu nastavíme. Etherchannel vychází z maximálního počtu portů, což je osm, a na každý port připadá poměr 1:1:1:1:1:1:1:1 hodnot, nebo toků viz následující tabulka.

Tabulka 1.1: *Rozložení datových toků*

Počet portů	Rozložení portů pro vyvažování	Datové toky na port
8	P1:P2:P3:P4:P5:P6:P7:P8	1:1:1:1:1:1:1:1
7	P1:P2:P3:P4:P5:P6:P7:P1	2:1:1:1:1:1:1
6	P1:P2:P3:P4:P5:P6:P1:P2	2:2:1:1:1:1
5	P1:P2:P3:P4:P5:P1:P2:P3	2:2:2:1:1
4	P1:P2:P3:P4:P1:P2:P3:P4	2:2:2:2
3	P1:P2:P3:P1:P2:P3:P1:P2	3:3:2
2	P1:P2:P1:P2:P1:P2:P1:P2	4:4

Z tabulky je vidět, že rovnoměrného poměru hodnot (toků) vyvážení získáme pouze, když budeme mít v zapojení Etherchannel 8,4 nebo 2 fyzické porty. Pokud zvolíme šest portů, tak dva z nich budou mít přiřazeny dvě hodnoty (toky), a tudíž budou více vytíženy než zbylé čtyři porty. Volba výběru následujícího portu, který bude mít přiřazen další tok, se řídí principem round-robin. Například pokud máme pět portů v Etherchannel, tak šestý tok bude opět přiřazen prvnímu portu, sedmý druhému a osmý třetímu, viz předchozí tabulka.

Pokud jsou v Etherchannel portu pouze dva porty, tak se rozhoduje na základě posledního bitu, protože pomocí jednoho bitu jsme schopni určit dvě hodnoty. Pokud jsou v Etherchannel 3 porty, tak aby se dokázali rozlišit, bude potřeba dvou bitů, stejně tak pro 4 porty. Více než 4 porty v Etherchannel bude potřeba rozlišit pomocí tří posledních bitů. Porty v Etherchannel jsou očíslovány od 0 do 7 (binárně 000 - 111)

Rozhoduje se na základě nejnižších (pravých) bitů v MAC adrese, nebo IP adrese, nebo TCP/UDP portech. Je-li rozhodováno jen na základě jedné hodnoty ze src nebo dst metody, tak hodnota rozhodujících bitů přímo označuje port, přes který bude provoz odeslán.

Je-li rozhodováno na základě kombinace dvou hodnot jako jsou src-dst-ip, src-dst-mac, src-dst-port, provede se nad skupinami rozhodujících bitů operace XOR jejíž výsledek označuje odchozí port. Následující tabulka znázorňuje operace nad zvolenými metodami.[3]

Tabulka 1.2: *Určení operací*

Metoda	Hash Operace	model přepínače
src-ip	bity	všechny
dst-ip	bity	všechny
src-dts-ip	XOR	všechny
src-mac	bity	všechny
dst-mac	bity	všechny
src-dst-mac	XOR	všechny
src-port	bity	4500-6500
dst-port	bity	4500-6501
src-dst-port	XOR	4500-6502

1.4 Výpočet vyvažování zátěže

Příklad src-dst-ip vyvažovací metody na Etherchannel tvořící třemi porty. Z předchozí tabulky č. 1.1 víme, že porty budou mít přiřazené hodnoty v poměru 3:3:2, takže dva porty budou mít po třech hodnotách (tocích) a jeden port bude mít dvě hodnoty (toky). Rozhodující budou dva poslední bity, protože pomocí dvou bitů jsme schopni oadresovat tři porty. Hodnoty se přiřazují způsobem round-robin, takže v případě tří portů přiřadíme čtvrtou hodnotu opět prvnímu.

Paket jdoucí z IP adresy 192.168.1.14 -> 11000000.10101000.00000001.00001110 [bin]

Na cílovou adresu 172.31.17.46 -> 10101100.00011111.00010001.00101110 [bin]

Použita src-dst-ip metoda

src IP: 192.168.1.14 (14 = 110[bin])

dst IP: 172.31.67.46 (16 = 110[bin])

operace XOR -> 000

Tabulka 1.3: *Výběr portu src-dst-ip*

		Pořadové číslo portu	port 1.	port 2.	port 3.
8 portů-8 hodnot	000	1.	000		
	001	2.		001	
	010	3.			010
	011	1.	011		
	100	2.		100	
	101	3.			101
	110	1.	110		
	111	2.		111	

Podle tabulky č. 1.3 lze vidět, které toky budou proudit kterým portem. Podle metody src-dst-ip na základě daných IP adresách budou data proudit portem číslo jedna. Kdyby přišel další tok se stejnou hodnotou hash výpočtu x00, tak bude použit port číslo 2, protože port jedna už je využitý a port dva má ve svém označení taky 00. Obdobně se budou počítat metody s více porty.

Metoda Src-IP na pěti portech:

Paket jdoucí z IP adresy 192.168.1.12 -> 11000000.10101000.00000001.00001100 [bin]

Na jakoukoliv cílovou adresu. Pro rozlišení budou potřeba poslední tři bity. Bity v src metodě rovnou určují daný port, neprovádí se hash operace.

Tabulka 1.4: *Výběr portu src-ip*

		Pořadové číslo portu	port 1.	port 2.	port 3.	port 4.	port 5.
8 portů-8 hodnot	000	1	000				
	001	2		001			
	010	3			010		
	011	4				011	
	100	5					100
	101	1	101				
	110	2		110			
	111	3			111		

Paket jdoucí z adresy 192.168.1.12 s hodnotou 100 bude poslán portem číslo pět.[4]

Etherchannel můžeme vytvořit pouze mezi dvěma síťovými prvky, přepínači, směrovači nebo Etherchannel mezi serverem a přepínačem, ale nemůžeme posílat provoz z jednohosměrovače, přepínače, nebo serveru do dvou rozdílných síťových prvků napříč jedním Etherchannel.

Tuhle techniku podporují přepínače vyšších řad a nazývá se Multi-Chassis Link Aggregation (M-LAG), každý výrobce používá svou implementaci MLAG, například Cisco nabízí virtual PortChannel (vPC), Virtual Switching Systems (VSS), HP nabízí Intelligent Resilient Framework (IRF). Jedna Etherchannel linka musí vždy propojovat dvě zařízení. Každý fyzický port Etherchannel linky musí mít stejnou konfiguraci na obou stranách obou zařízení. Etherchannel technologie sjednocuje pouze porty stejného typu. Máme-li některé porty Fastethernet a Gigabitethernet musíme srovnat jejich rychlosti, musíme přepnout vyjednávání na Gigabitethernet rozhraní na 100Mbit/s (Fastethernet). Na L2 přepínači je Etherchannel použit k agregaci access portů nebo trunk portů. Například: fyzické porty nakonfigurovány jako trunk na straně jedné musí být stejně nakonfigurovány i na straně druhé. Každý Etherchannel je logický port, konfigurace na logickém portu je automaticky použita na všechny fyzické porty uvnitř Etherchannel. Etherchannel vytváří agregaci fyzických linek, které se jeví jako jedna logická linka. Pokud existuje několik Etherchannel spojení mezi dvěma přepínači tak STP zablokuje jednu z redundantních linek, tahle blokace se týká všech fyzických portů patřící do jednoho Etherchannel.

1.5 Link Aggregation Control Protocol (LACP):

Jedná se o IEEE specifikaci (802.3ad), která umožňuje několika fyzickým portům být součástí jednoho logického kanálu s názvem Etherchannel. LACP protokol umožňuje směrovači, nebo přepínači automaticky vyjednat kanál zasíláním LACP paketů sousedovi. V okamžiku kdy jsou porty nakonfigurovány pomocí LACP, tak se zařízení snaží spustit maximální možný počet portů do Etherchannel svazku, případně můžeme maximální počet portů nastavit manuálně. Při konfiguraci LACP protokolu Cisco přepínač nabízí tři módy ve kterých umí pracovat:

- passive - Umísťuje port do pasivního vyjednávacího stavu, ve kterém pouze odpovídá na LACP pakety které přijal, neiniciuje spojení.

- active - Mód, který umísťuje port do aktivního vyjednávacího stavu, kdy rozesílá LACP pakety na sousední porty.

- on- Všechny porty kanálu (které neběží v LACP, ani PaGP) znamenají tenhle mód. Je to mód, který vynutí LAN port pro Etherchannel bezpodmínečně. V módu on je použitelný port, pouze pokud je ve skupině s dalším portem, který je v módu on, jinak se jedná o normální port. Porty nastavené v módu on nezasílají vyjednávací provoz do sousedních portů. Nemůžeme nastavit mód on na jednom prvku a na druhém Etherchannel pomocí LACP, nebo PagP protokolem. Pokud jedna strana používá on mód, druhá strana musí také. Výchozí nastavení port-channel je on.

Nepovinné parametry, které mají výchozí přednastavení:

- Systém ID: Hodnota použitá pro jednoznačnou identifikaci přepínače. Systém ID také slouží jako prioritní hodnota, která umožňuje sousedním směrovačům propojeným Etherchannel , aby rozhodla, která konfigurace přepínače bude mít prioritu. Systém ID je tvořen kombinací Systém priority a MAC adresou. Menší hodnota znamená vyšší prioritu.

- System priority: Každý přepínač s běžícím LACP musí mít system priority. System priority může být nastaven automaticky, nebo pomocí příkazu v CLI. Přepínač používá MAC adresu a systém priority k sestavení system ID. Slouží k určení vyjednávání, který z přepínačů bude mít hlavní slovo při výběru aktivních a záložních portů. Čím nižší číselná hodnota tím vyšší priorita. Pokud budou mít oba přepínače stejnou System prioritu, tak bude rozhodovat Systém ID o tom, kdo bude mít hlavní slovo.

- Port priority: Každý port na přepínači musí mít port priority. Přepínač používá port priority k rozhodnutí stavu portu, jestli bude v pohotovostním módu nebo bude aktivně využíván. Může být také nastaveno automaticky, nebo pomocí CLI. Port priority a port number tvoří jednoznačný identifikátor portu. Port s vyšší prioritou (menší hodnotou) bude zvolen jako aktivní. Výchozí hodnota je 32768. [5]

1.6 Port Aggregation Protocol (PAgP)

PAgp je proprietární síťový protokol vytvořený firmou Cisco Systems, který se používá pro automatizovanou logickou agregaci portů přepínače do Etherchannel. To znamená, že může být použita pouze mezi Cisco přepínači nebo přepínači od licencovaných výrobců. Má podobný účel jako protokol LACP (802.3ad), PAgP pakety jsou zasílány každých 30 sekund. PAgP kontroluje konfiguraci konzistence a stará se o přidávání linek a výpadky mezi dvěma přepínači. Nabízí módy s jinými názvy ale stejnou funkcionalitou.

- auto- Umísťuje port do pasivního vyjednávacího stavu, ve kterém pouze odpovídá na PaGP pakety které přijal, neiniciuje spojení.

- desiderable - Mód, který umísťuje port do aktivního vyjednávacího stavu, kdy rozesílá PaGP pakety na sousední porty.

- on Nejsou použity žádné protokoly, je použit manuální režim

Vytvoříme-li Etherchannel pomocí LACP, PAgP nebo manuálně, tak STP a jeho další varianty vidí Etherchannel jako jednu linku, tudíž může buďto blokovat všechny fyzické porty v Etherchannel, nebo je všechny nechá povolené.[1]

Tabulka 1.5: *Komparace protokolů*

Protokol	přepínač A	přepínač B	výsledek vyjednání
PAGP	Auto	Auto	bez vyjednání
	Auto	Desiderable	Vyjednání úspěšné
	Auto	On	bez vyjednání
	Desiderable	Desiderable	Vyjednání úspěšné
LACP	Passive	Passive	bez vyjednání
	Passive	Active	Vyjednání úspěšné
	Passive	On	bez vyjednání
	Active	Active	Vyjednání úspěšné

1.7 Zabránění smyčkám na linkové vrstvě

Pro následující možnosti redundance na druhé vrstvě bude dobré si ve zkratce popsat, jaké jsou techniky k zabráněním smyčkám.

1.7.1 Spanning tree protocol (STP)

Spanning tree protokol pracující na druhé vrstvě na přepínačích a mostech (bridge). Specifikace pro STP je IEEE 802.1d. Hlavním účelem STP je zajištění sítě bez smyček. Pokud máme redundantní zapojení mezi několika přepínači, tak vznikají smyčky, které mají neblahý vliv na fungování sítě. STP vypočítá hodnoty cest ke kořenovému přepínači a nadbytečné linky zablokuje. Pokud dojde k rozpojení některé neblokované linky, tak STP přepočítá cesty a povolí nějakou z blokovaných cest a tím umožní opětovné dostupnosti všech prvků. Můžeme říct, že pracuje nad jednou nativní VLAN 1.

1.7.2 Rapid Spanning tree protocol (RSTP)

Evoluce původního STP, hlavními znaky jsou rychlá konvergence a více stavů portů.

1.7.3 Per-VLAN Spanning Tree (PVST)

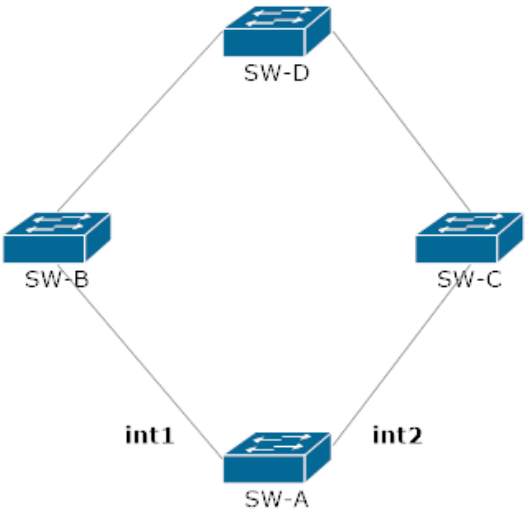
Proprietární Cisco řešení, vychází z IEEE 802.1d STP, ale pro každou VLAN běží samostatná instance STP. Výhodou je, že mohou rozdělit zátěž, že každá VLAN komunikuje jinou cestou. Nevýhodou je větší zatížení přepínače, protože pro každou VLAN počítá STP instanci. Používá ISL trunk pro zapouzdření VLAN.

1.7.4 Multiple Spanning Tree (MSTP)

(MSTP) - IEEE 802.1s standard inspirovaný Cisco proprietárním protokolem Multiple Spanning Tree Protocol (MSTP). Rychlé jako RSTP a umožňuje mapovat několik VLAN do jedné STP instance. Tímto umožní ušetřit počet STP pro velký počet VLAN a současně redukuje zatížení výpočtů. Používá se na páteřní sítě. Revizí v roce 2003 byl sloučen do normy 802.1q, která se věnuje VLAN.[6]

1.8 Huawei proprietární technika

Huawei plným názvem Huawei Technologies Co. Ltd., je mezinárodní telekomunikační společnost, dodavatel informačních a komunikačních řešení, se sídlem v čínském Šen-čenu. Podle obratu byla roku 2010 největší čínskou a druhou největší světovou společností (za společností Ericsson) vyrábějící telekomunikační zařízení, a v roce 2012 se stala jedničkou. Během roku 2014 se dostala z pátého na třetí místo v prodeji chytrých telefonů (prodal jich 75 milionů). Huawei přepínač nabízí možnost redundantního zapojení bez STP a současně bez smyček. Smart link je proprietární technika značky Huawei, která nabízí rychlé přepnutí mezi dvěma rozhraními, kdy jedno pracuje jako aktivní a druhé jako záložní. Smart link je použit v dual-homed sítích k zajištění efektivního a rychlého přechodu. Pokud je přepínač připojen pouze jednou linkou k nadřazeným prvkům, takzvanou "uplink" linkou, tak služby, nebo tok dat mohou být přerušeny, pokud dojde k selhání jednoho bodu, jedné linky. V zapojení dual-homed sítích je tomu jinak, zapojení dvou uplink linek redukuje dopad výpadku jedné z nich a tím zvyšuje spolehlivost sítě.



Obrázek 1.4: *Dual homed zapojení*

Jak je na obrazku 1.4, přepínač SW-A je ve vztahu dual-homed k přepínači SW-B a SW-C pomocí dvou linek. Jedna linka je zálohou druhé. Nicméně zde se projevuje smyčka přepínačů A ->B ->C->D->A, která způsobí broadcast storm.

Obvykle se používá Spanning Tree Protokol (STP) k zabránění smyček. Nicméně dlouhá doba konvergence STP může způsobit ztrátu mnoha paketů. STP není použitelný v sítích kde je požadována rychlá konvergence. Další „proti smyčková“ možnost je použití další proprietární technologie Huawei Rapid Ring Protection Protocol (RRPP), která nabízí rychlejší konvergenční časy. Nicméně RRPP se používá v komplexních kruhových sítích a jeho konfigurace je náročná. Jelikož se jedná o proprietární technologii tak jej není možno nasadit na Huawei – Cisco zapojeních. Huawei nabízí Smart Link řešení k zabránění takových smyček v dual-homed sítích, které může pracovat i s přepínači jiných výrobců.

Výhody:

Když oba uplink porty pracují v pořádku, tak jeden z nich je aktivní (Master) a je v přeposílacím režimu a druhý zůstává v neaktivním (Slave) k zabránění smyčky. Nicméně port není zcela vypnutý, protistrana hlásí, že má stav portu „UP“. Smart Link přepínač má pouze blokovaný port. V porovnání s protokolem STP Smart Link nabízí o mnoho řádů rychlejší konvergenci. Když aktivní port selže, tak je provoz přehozen na neaktivní port v milisekundách. Smart Link zlepšuje spolehlivost pomocí zálohování mezi dvěma porty. Smart Link také používá Flush paket a Smart Link instanci k implementaci rychlého přepnutí a vyvažování zátěže.

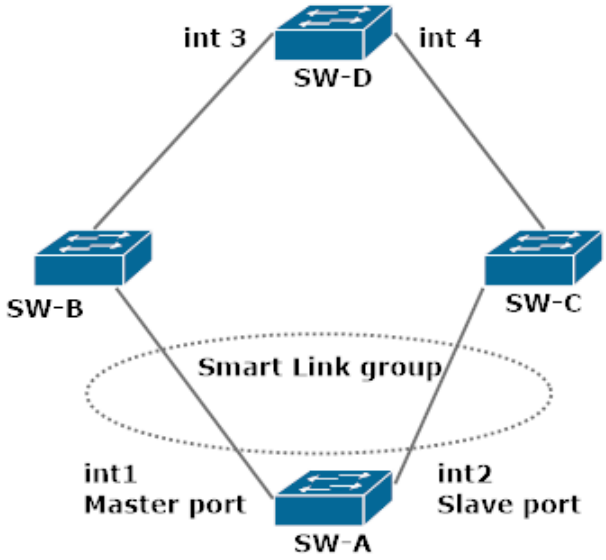
Nevýhody:

Smart Link pouze detekuje stav linky UP/DOWN.

Neumí detekovat jednosměrný provoz.

Neumí detekovat, jestli port není zablokován pomocí STP, nebo hardwarovou chybou.

Hrozí riziko smyček při neodborné konfiguraci.



Obrázek 1.5: *Smart Link group*

1.8.1 Základní koncept Smart Link

Master port, obrázek č.1.5 ve Smart Link skupině je rozhraní, které jako první přechází do aktivního stavu. Master port není vždy aktivní, když selže, tak je provoz přesměrován na druhý port, Slave port se stává aktivním. Master port zůstává neaktivní až do dalšího přepnutí, i když je porucha opravena již před přepnutím. Služby jsou přepnuty na Master port až po vypršení intervalu selhání.

1.8.2 Flush Packet

Pokud dojde k přepojení aktivní a neaktivní linky Smart Link skupiny tak dojde k tomu, že stávající směrovací záznamy se již nebudou vztahovat k nové topologii. Všechny záznamy MAC adres a Address Resolution Protokol (ARP) se musí aktualizovat. Proto Smart Link zasílá takzvané Flush pakety s žádostí o aktualizaci MAC tabulek a ARP záznamů. Na obrázku č. 1.5 když dojde k přepojení ve skupině Smart Link, tak přepínač SW-A zasílá Flush paket s žádostí na SW-C, SW-D, SW-B aby si aktualizovali MAC a ARP. Flush pakety jsou zasílány pomocí broadcast vysílání.

1.8.3 Control VLAN

Control VLAN je označení VLAN pro zasílání Flush paketů pomocí broadcast vysílání. Jak je na obrázku č. 1.5, pokud přepínač SW-A má nastaveno zasílání Flush paketů, tak zasílá Flush pakety pomocí broadcast vysílání nově aktivní linkou. Uplink přepínače používají kontrolní VLAN pro příjem a zpracování Flush paketů. Pokud dojde k přepojení na přepínači SW-A tak si uplink přepínače pomocí Flush paketu aktualizují své MAC a ARP tabulky.

1.8.4 Aktualizace tabulek

1.8.4.1 Automatické aktualizace založena na provozu

Tahle metoda je použita když nadřazené uplink zařízení nepodporují Smart Link funkci. Tím mohou být CISCO, Zyxel a mnoho dalších. Tyhle zařízení si aktualizují MAC a ARP tabulky na základě provozu dat. Pokud není žádný odchozí provoz směrem z přepínače SW-A do ostatních, tak přepínač SW-D bude na přepínač SW-A posílat data skrze port 3. Tudíž pakety se k přepínači SW-A nedostanou, což znamená ztrátu dat. Provoz bude směrován na SW-A správným portem až budou záznamy v MAC a ARP tabulce aktualizovány, nebo smazány pomočí časovačů.

1.8.4.2 Automatická aktualizace založena na časovačích

MAC a ARP záznamy na přepínači SW-D jsou neaktuální, proto SW-D nemůže zasílat data správným portem. Jakmile vyprší flush časovač a záznamy se smažou, tak přepínač začne zasílat pakety všemi porty kromě příchozího. Poté se z příchozí odpovědi od přepínače SW-A portem int 4 dozví správnou cestu. Paket je tedy následně směrován na SW-A přes SW-C.

1.8.5 Zasílání Flush paketů

Tahle možnost se nabízí, pokud všechny ostatní přepínače taky podporují Smart Link funkci a umí pracovat s Flush pakety, tudíž musí být taky značky Huawei. K implementaci rychlého přepojení se na přepínači SW-A povolí služba zasílání Flush paketů. Také přepínače, které tvoří uplink linky pro SW-A musí být nastaveny, aby přijímali Flush pakety. Postup chování při správně nakonfigurovaném zasílání a přijímání Flush paketů je následující:

- Jakmile dojde k přepojení na přepínači SW-A, tak SW-A zasílá Flush pakety skrze novou aktivní linku int2.

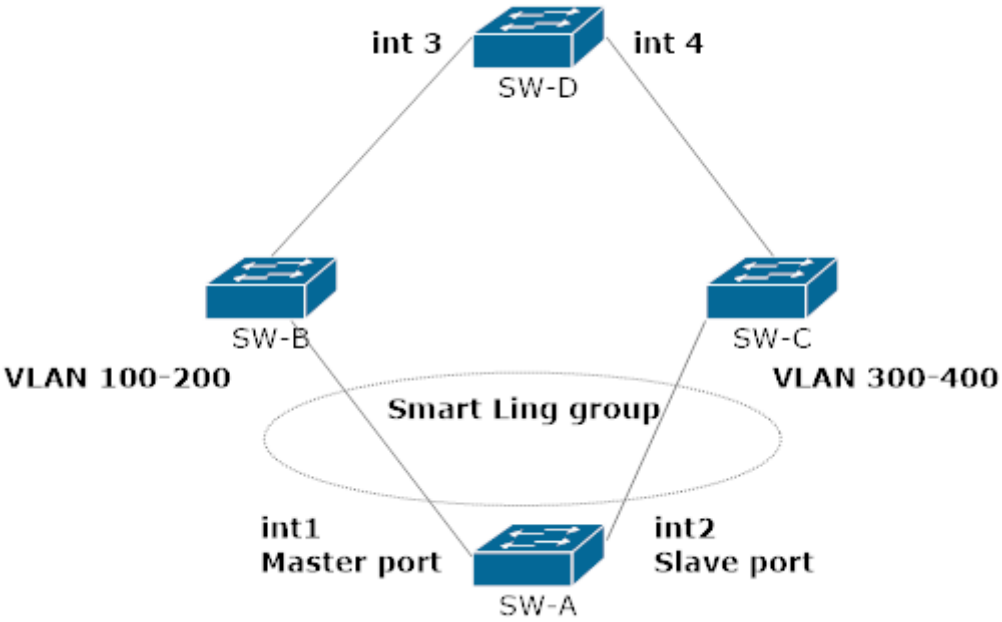
- V okamžiku kdy přijme přepínač SW-C Flush paket, tak jej zpracuje, aktualizuje si tabulky a zasílá dalším rozhraním na SW-D.

- Jakmile přijdou na SW-D data směrující pro přepínač SW-A, tak je zasílá na základě nově aktualizovaných záznamů v tabulkách. Tímto směrem budou data zaslány správně. Flush pakety spouští na nadřazených přepínačích aktualizaci MAC adres a ARP záznamů předtím, něž vyprší jejich doba existence, tím se redukuje čas aktualizace.

1.8.6 Vyvažování zátěže

Obvykle přepínač, který potřebuje zasílat data ve více VLAN bude používat jeden aktivní port pro zasílání dat a druhý jako záložní, který bude v neaktivním stavu a tudíž nebude posílat žádná data. Smart Link podporuje vyvažování zátěže, které umožňuje zasílání dat z různých VLAN pomocí různých portů. Vyvažování zlepšuje využití portů s funkcí zálohy jednoho portu

druhým. Jakmile je nastavena instance vyvažování zátěže na Smart Link skupině, záložní port najednou bude přeposílat také data, a to z VLAN které budou specifikované v instanci MST. Technika vyvažování zátěže staví na Multiple Spanning Tree (MST) protokolu, kdy se různé VLAN stávají součástí různé instance.



Obrázek 1.6: *Vyvažování zátěže*

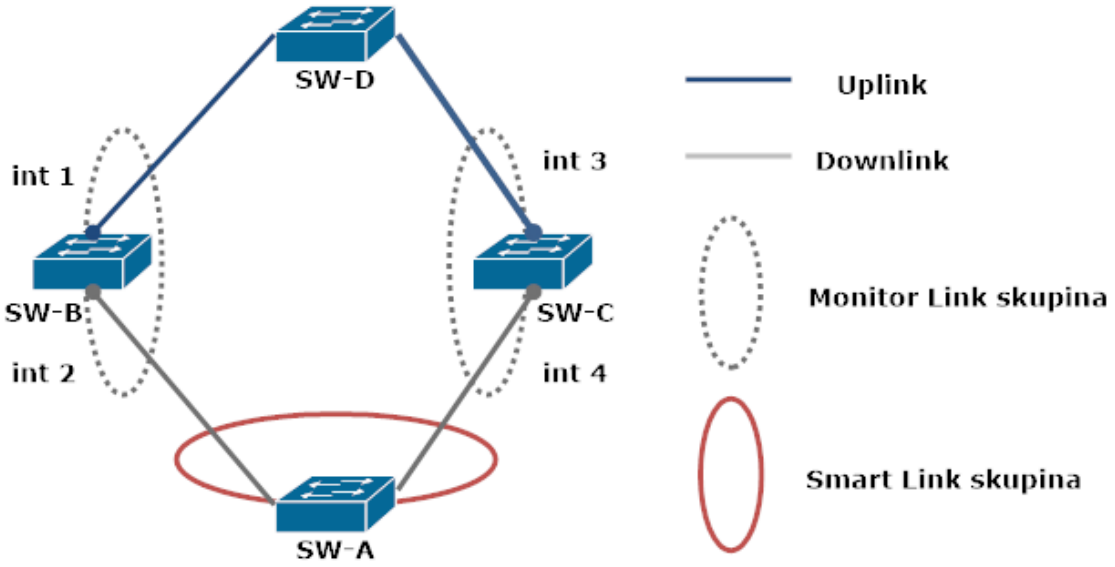
Ke zvýšení využití obou portů nastavíme instanci vyvažování zátěže, kterou spojíme s rozsahem VLAN 300 až 400, poté ji spojíme se Slave portem int2. Následně se bude dít to, že VLAN asociované s portem Slave budou tímto portem procházet. Zbylé VLAN, které nejsou asociované s žádnou instancí, se budou zasílat skrze port int 1.

1.8.7 **Monitor Link**

Monitor Link je mechanismem pro monitorování uplink portu a ovládání jednoho nebo několika downlink portů. Člen Monitor Link skupiny může být port, Etherchannel pomocí LACP, nebo manuální, nebo Smart Link skupina.

V situaci kdy dojde k výpadkům na uplink portu přepínače SW-B int 3, tak Monitor Link požádá downlink zařízení, což je v našem případě SW-A, k přepnutí z aktivního na záložní port. Podle obrázku 1.7 je Smart Link skupina nakonfigurována na přepínači SW-A, který má port int 1 nastaven jako Master a port int 2 jako Slave. Dále je nastaven Monitor Link na přepínači SW-B . V okamžiku, kdy aktivní linka připojená k int 1 spadne, tak okamžitě přepínač SW-A nastaví Slave port int 2 jako aktivní. Když ale uplink port int 3 přepínače SW-B spadne, tak přepínač SW-A nemá možnost tuhle situaci detekovat, protože přímo připojená linka na port int 1 je stále ve funkčním stavu. Smart Link nedokáže odhalit tento výpadek. Dochází k přerušení komunikace, protože pakety nemohou být poslány na int 1 přepínače SW-A.

Výhody: Monitor Link může být spojen se Smart Link technikou k dosažení větší oblasti působnosti.



Obrázek 1.7: *Smart Link a Monitor Linki*

Uplink rozhraní je monitorováno v reálném čase downlink rozhraními v Monitor Link skupině. Pokud uplink rozhraní spadne, tak Monitor Link skupina všechny nadefinované downlink rozhraní vypne. Jakmile uplink bude opět funkční, tak Smart Link skupina nahodí všechny nadefinované downlink porty. Downlink rozhraní monitorují uplink porty nacházející se v Monitor Link skupině. Výpadek downlink portu nemá žádný vliv na uplink porty nebo další downlink porty. [7]

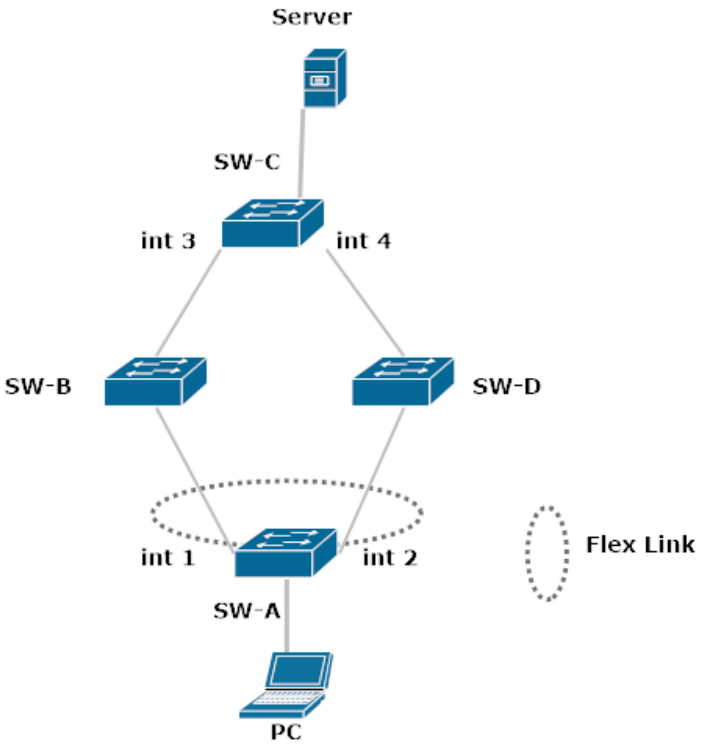
1.9 CISCO proprietární technika

1.9.1 Flex Links

Flex Link je obdobná technika Smart Link u značky Huawei, skládá se pomocí páru dvou rozhraní (portů nebo Ether Channel), kde jedno pracuje jako záloha toho druhého. Pokud aktivní rozhraní selže, přebírá záložní rozhraní funkci přeposílání dat. Flex link je typicky konfigurován v dual-homed sítích, kde není žádoucí nasazovat pomalé STP. Flex Link nabízí redundanci na L2 vrstvě jako alternativu k STP.

1.9.2 MAC address-Table Move Update

Stejně jako Flush pakety u Huawei má i CISCO své informační pakety k aktualizaci tabulek. Funkce MAC address-table umožňuje přepínačům poskytnout rychlou obousměrnou konvergenci, když dojde k přepnutí aktivního a záložního portu.



Obrázek 1.8: *Flex Link*

Podle obrazku č. 1.8 Přepínač SW-A je přístupový přepínač a má porty int 1 a int 2 připojeny k uplink přepínačům SW-B a SW-D pomocí Flex Link páru. Port int 1 je ve stavu přeposílání dat a port int 2 je v neaktivním jako záloha. Data jdoucí z počítače k serveru jsou směrovány z portu int 1 na port int 3 přepínače SW-C. MAC adresa počítače je naučená na portu int 3 přepínače SW-C. Data jdoucí ze serveru na počítač jsou směrovaná z portu SW-C int 3 na port SW-A int 1.

Berme v úvahu, že MAC address-table funkce není nakonfigurována. Stane se následující scénář. Pokud port int 1 selže, tak se port int 2 stává aktivním a přeposílá data. Nicméně ještě nějakou dobu přepínač SW-C si bude držet záznam MAC adresy počítače na portu 3. Tudíž počítač nedostane žádné data, protože port 1 již není aktivní. Pokud přepínač SW-C smaže záznam MAC adresy počítače na portu int 3 a nasadí ho na port 4, tak data jdoucí ze serveru budou téct přes port 4 na SW-D.

Pokud bude MAC address-table funkce nakonfigurována a spuštěna na přepínačích, tak se odehraje následující scénář. Pokud port int 1 selže Přepínač SW-A zašle MAC address-table

přes port int 2. Přepínač SW-C dostane tuhle zprávu na portu 4 a okamžitě si vytvoří záznam pro počítač na portu int 4, což redukuje čas konvergence.

1.9.3 Flex link vyvažování zátěže

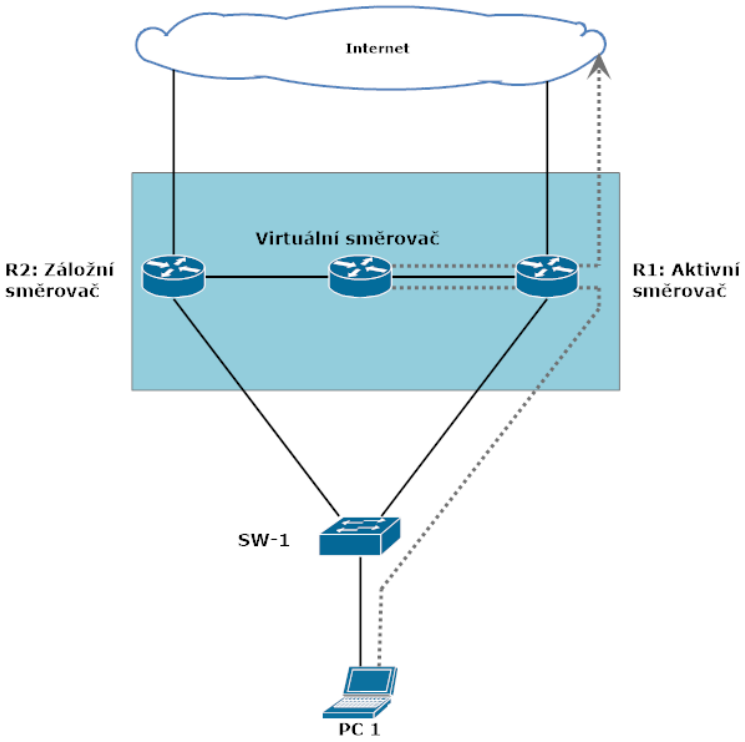
VLAN Flex Link vyvažování zátěže umožňuje konfiguraci Flex Link páru portů k současnému přeposílání dat oběma porty. Například nastavíme 1 - 100 VLAN, tak prvních 50 VLAN bude přeposíláno prvním portem a zbytek bude přeposílán druhým portem. Pokud jeden port selže, tak záložní aktivní port bude přeposílat všechny VLAN, tedy i ty, které byly nadefinovány na neaktivním portu. Tímto způsobem kromě poskytnutí zálohy a vyšší dostupnosti může Flex Link být použit pro vyvažování zátěže. Navíc vyvažování zátěže neuplatňuje žádné omezení pro uplink přepínače.[8]

1.10 Redundance na síťové vrstvě

Klientské stanice, stejně jako servery nemají uloženy všechny směrovací informace o internetu ve vlastní lokální směrovací tabulce. Ani to není jejich povinností, takovou povinnost zastávají směrovače. Pokud se nachází partner komunikace klientské stanice nebo serveru mimo lokální síť, tak s pomocí ARP dotazu klientská stanice nebo server neuspěje. Zde nastává hlavní role takzvané výchozí brány, která má za úkol všechny takové dotazy zprostředkovat a přeposlat dál správným směrem. Protože výchozí brány zajišťují klíčovou roli v takové komunikaci mezi sítěmi, je jejich dostupnost prvořadá. V případě že směrovač jako výchozí brána vypoví službu, bude se muset u všech dotčených stanic přenastavit IP adresa výchozí brány na alternativní, což může v rozsáhlých sítích znamenat problém. Poskytnutím redundantních bran je řešení, jak se takovému problému vyhnou. K zajištění takové funkcionality musíme mít správně nakonfigurován takzvaný protokol redundantního prvního skoku „first hop redundancy protocol“ značeno FHRP, jejich implementací jsou: VRRP(Virtual Router Redundancy Protokol), CISCO proprietární protokoly HSRP(Hot Standby Routing Protocol) a GLBP (Gateway Load Balancing Protocol). S jejich pomocí klientské stanice ani nemusí tušit, že někde došlo k odstavení výchozí brány.

1.11 Virtual Router Redundancy Protocol (VRRP)

Jedná se o otevřený standart, který používají směrovače pro komunikaci mezi sebou, slouží pro zálohování provozu pomocí redundantních směrovačů. Nejedná se o vyvažování zátěže, a proto síťový provoz prochází právě jedním směrovačem. Tomuto směrovači říkáme master, resp. vlastník. V případě jeho vypadnutí ho zastoupí záložní směrovač „backup router“, ze kterého se stane master, záložních směrovačů může být více. Pomocí takové techniky se sníží doba výpadku.



Obrázek 1.9: *VRRP zapojení*

VRRP specifikuje protokol volby, který dynamicky přiřazuje odpovědnost přeposílání paketů z jednoho směrovače na druhý, když první selže. VRRP směrovač, který má nastavenu IP adresu stejnou s virtuálním směrovačem se nazývá Master a předává dál pakety odeslané na tuto virtuální IP adresu. Volební proces VRRP poskytuje dynamické převzetí zodpovědnosti pro přeposílání když Master selže. To umožňuje jakoukoliv adresu virtuálního směrovače v síti použít jako první „defaultní“ skok.

1.11.1 Volba Master směrovače

Volba Master směrovače se provádí, protože jen jeden směrovač může ve VRRP skupině být aktivním. Ostatní směrovače zůstávají se stavu záložního směrovače. Master se určuje pomocí priority, čím vyšší hodnota, tím větší priorita. Pokud má směrovač nastavenu stejnou fyzickou IP adresu jako je adresa virtuálního směrovače, tak se automaticky stává Masterem. Ve výchozí konfiguraci když není nastavena priorita manuálně, tak se použije výchozí hodnota rovna 100. Pokud směrovače mají stejnou prioritu, což se s výchozím nastavením priority stává, tak se volí Master podle vyšší IP adresy. Priority hodnota rovna nule znamená, že Master již nechce být součástí v VRRP. Je to použito proto, aby rychleji záložní směrovač reagoval a stal se Masterem, než kdyby čekal, až vyprší jeho časovač Hold-time.

1.11.2 VRRP preemption

VRRP nabízí možnost volby takzvané “preemption“ což znamená, že pokud se havarovaný Master směrovač po havárii opět probral, tak přebírá zodpovědnost za provoz svou vyšší prioritou a původně záložní se opět stává záložním. V případě kdybychom preemption nenastavili, tak původně záložní směrovač, který se stal aktivním, bude po celou dobu aktivním, dokud také neselže.

1.11.3 Advertiement pakety

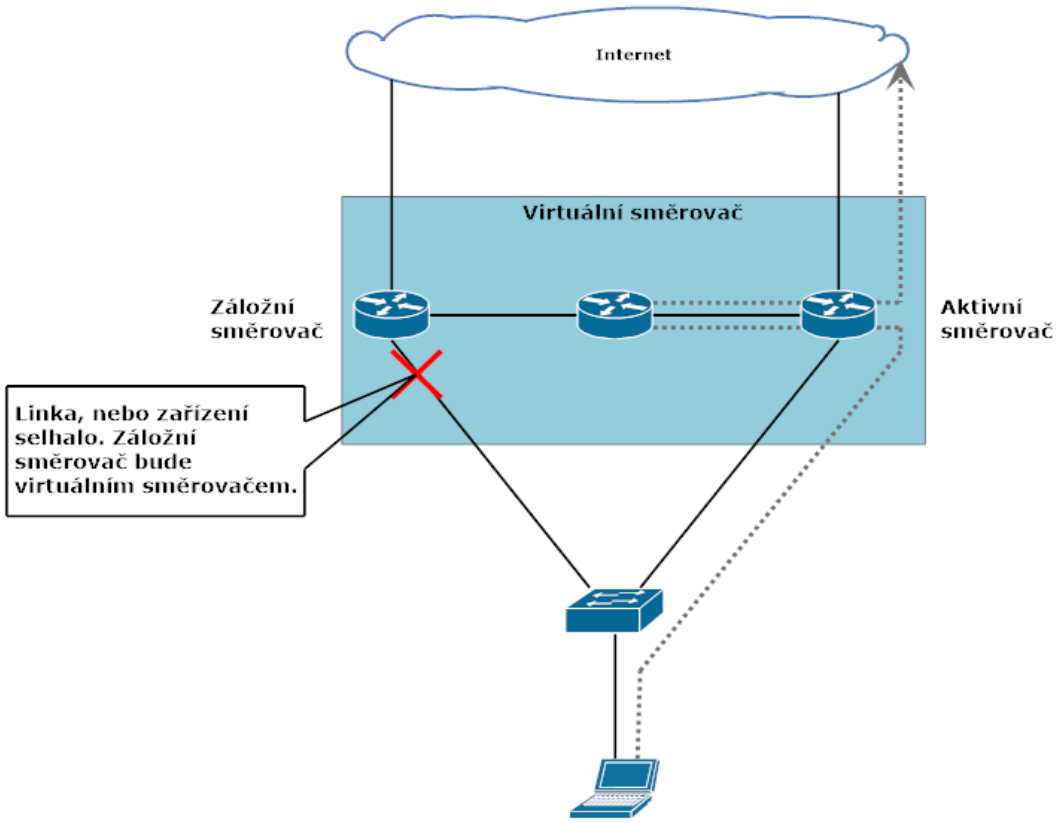
Master směrovač pravidelně rozesílá takzvané advertisement pakety, pomocí kterých informuje ostatní směrovače, že je stále v provozu. Pokud dojde k tomu že Master v definovaném čase „hold-time“ neodešle advertisement paket, tak záložní Backup směrovač převezme IP a MAC adresu virtuálního směrovače. Pokud máme v síti více VLAN můžeme vhodnou konfigurací nastavit určitý typ vyvažování zátěže, za předpokladu že naše směrovače a přepínače podporují technologii multiple spanning tree protocol MSTP. [1]

1.12 Hot Standby Router Protocol (HSRP)

HSRP je redundantní protokol vyvinut společností Cisco k poskytnutí redundance výchozích bran bez přidávání konfigurace na koncových zařízeních sítě. S nastavením HSRP mezi několika směrovači mohou směrovače pracovat společně a tím se prezentovat jako jeden virtuální směrovač pro koncové stanice, jako na následujícím obrázku. Sdílením jedné IP adresy a jedné MAC adresy mohou dva a více směrovačů vystupovat jako jeden virtuální směrovač, jak je tomu u VRRP.

IP adresa virtuálního směrovače bude nastavena jako výchozí brána na koncových stanicích dané sítě. Než jsou rámce odesílány na výchozí bránu, tak se koncová stanice dotazuje pomocí ARP protokolu pro zjištění MAC adresy k IP adrese výchozí brány. ARP odpověď vrací MAC adresu virtuálního směrovače. Rámce zaslané na MAC adresu virtuálního směrovače jsou fyzicky zpracovány aktivním směrovačem, který je součástí takzvané. „virtual router group“. Fyzický směrovač, který propouští provoz je transparentní pro koncové stanice.

HSRP poskytuje mechanismus pro určení, který směrovač bude v aktivní roli přeposílání provozu, také obsahuje mechanismus pro určení, kdy je třeba, aby aktivní roli převzal záložní směrovač. Přechod z jednoho přeposílajícího směrovače na druhý je transparentní pro koncové stanice. Například když aktivní směrovač, nebo linky mezi směrovači selžou, tak záložní směrovač přestane přijímat „hello“ zprávy od aktivního směrovače. Poté se záložní směrovač rozhodne převzít roli přeposílání a stává se z něj aktivní směrovač. Protože nový směrovač převzal aktivní roli, tak přijímá i IP adresu s MAC adresou virtuálního směrovače. Pro koncovou stanici nedochází k žádnému narušení provozu.



Obrázek 1.10: *Výpadek portu HSRP*

HSRP aktivní a záložní směrovače zasílají „hello“ zprávy po multicastové adrese 224.0.0.2 UDP port 1985. Všechny směrovače v HSRP skupině musí být v L2 vrstvě sousedé aby si mohli vyměňovat „hello“ pakety.

Všechny směrovače v HSRP skupině musí mít specifickou roli a specifické chování:

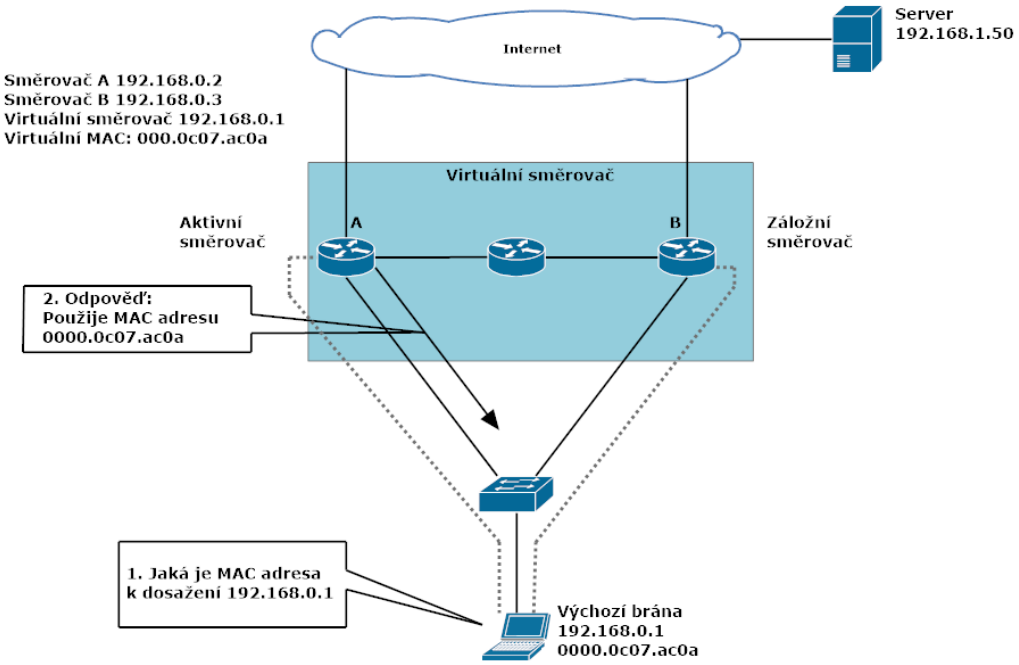
- Virtuální směrovač: Dvojice IP adresy a MAC adresy, které mají koncové stanice nastaveny jako defaultní bránu. Aktivní směrovač zpracovává všechny pakety a rámce, které jsou zaslány na adresu virtuálního směrovače. Vždy je pouze jeden virtuální směrovač ve skupině.

- Aktivní směrovač: V HSRP skupině je jeden směrovač zvolený jako aktivní. Aktivní směrovač fyzicky přeposílá pakety zaslané na MAC adresu virtuálního směrovače a odpovídá na ARP dotazy.

- Záložní směrovač: Poslouchá periodické „hello“ zprávy od aktivního směrovače. Když aktivní směrovač selže, tak ostatní směrovače ve stejné skupině přestanou přijímat „hello“ zprávy. Záložní směrovač se rozhodne převzít roli aktivního směrovače.

- Ostatní směrovače: Ve skupině může být víc než dva směrovače, ale pouze jeden může být aktivní a jeden nebo více záložních. Ostatní směrovače zůstávají v počátečním stavu, dojde-li k selhání obou: aktivního i záložního směrovače, tak se ostatní směrovače domluví, kdo bude aktivní a kdo záložní.

Směrovač A převzal aktivní roli a přeposílá všechny rámce adresované MAC adrese přiřazené HSRP skupině, tím je 0000.0c07.acXX kde XX je identifikátor skupiny.



Obrázek 1.11: *HSRP protokol*

Hot standby routing protocol nabízí více stavů v porovnání s protokolem VRRP:

Počáteční (Initial): Počáteční stav indikuje že HSRP neběží. Tento stav se stává pomocí změny konfigurace, nebo když se rozhraní zapíná.

Naslouchá (Listen): Směrovač zná virtuální adresu, ale není ani aktivní, ani záložní. Pouze naslouchá zprávy od těchto směrovačů.

Mluví (Speak): Směrovač vysílá periodické „hello“ zprávy a aktivně se podílí na volbě aktivního nebo záložního režimu směrovače. Směrovač se nemůže stát „mluvícím“ dokud nebude vědět IP adresu virtuálního směrovače.

Záložní (Standby): Směrovač je prvním kandidátem být v aktivním režimu, zasílá periodicky „hello“ zprávy. S výjimkou přechodových podmínek, je nanejvýš jeden směrovač ve skupině v záložním režimu.

Aktivní (Active): Směrovač předává rámce, které jsou odesílány na MAC adresu virtuální směrovače. Směrovač rozesílá periodicky „hello“ zprávy. S výjimkou přechodových podmínek, je nanejvýš jeden směrovač ve skupině v aktivním režimu

.

HSRP přechod stavů:

Všechny směrovače začínají v „initial“ stavu, který je startovní stav a indikuje že HSRP ještě neběží. Do tohoto stavu se přechází, když je rozhraní HSRP zakázáno, nebo když je port nastartován (pomocí příkazu no shutdown).

Úkolem naslouchacího stavu je určení, jestli jsou ve skupině již nějaké aktivní nebo záložní směrovače. V roli „speak“ se směrovače aktivně podílejí na výběru aktivního a záložního směrovače. HSRP používá „hello“ a „hold“ časovače k určení jestli se přepne do jiného stavu.

1.13 Gateway Load Balancing Protocol (GLBP)

GLBP je protokol podobný VRRP nebo HSRP protokolům, ale terminologie se liší a jeho chování je dynamičtější a robustnější. Zajišťuje automatickou zálohu výchozí brány díky redundantnímu zapojení směrovačů do sítě.

GLBP je Cisco proprietární řešení, které umožňuje automatický výběr a současné využití několika dostupných směrovačů. Zajišťuje také automatické převzetí služeb při selhání některé z těchto bran. Několik bran sdílí zátěž paketů, které se jeví z klientského pohledu jako zaslané na jednu IP adresu výchozí brány. GLBP řešení obsahuje dva druhy členů:

1.13.1 GLBP active virtual gateway (AVG)

Členové GLBP skupiny vyberou jednu bránu, která bude AVG pro tuhle skupinu. Volba je provedena na základě hodnoty priority, která je ve výchozím nastavení rovna 100, pokud mají stejnou prioritu členové GLBP skupiny, tak se rozhoduje na základě IP adresy, kde vyšší hodnota znamená vyšší prioritu. Ostatní členové zajišťují zálohu pro AVG pro případ, kdyby bylo nedostupné. AVG přiřazuje virtuální MAC adresu každému účastníkovi GLBP skupiny. AVG naslouchá na požadavky ARP dotazů klientů na IP adresu výchozí brány a odpovídá MAC adresou jednoho z účastníků. Tímto zajišťuje vyvažování zátěže mezi účastníky GLBP skupiny.

1.13.2 GLBP active virtual forwarder (AVF)

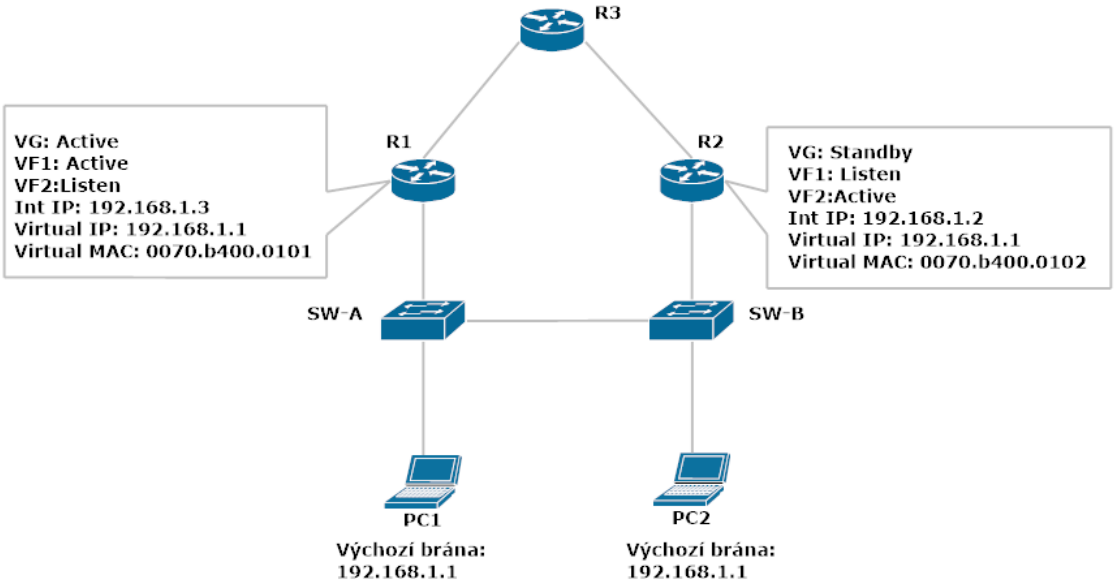
Je každá brána, která zodpovídá za přeposílání paketů směřovaných na virtuální MAC adresu, kterou jí přiřadil AVG. AVF bran může být maximálně čtyři v jedné GLBP skupině. AVF člen je současně i AVG. Ostatní členové GLBP skupiny jsou sekundární brány, které se nezúčastní přeposílání, dokud některé z AVF nevypoví službu. Všichni členové GLBP skupiny spolu komunikují pomocí "hello" zpráv, které jsou zasílány každé tři vteřiny na multicast adresu 224.0.0.102 s UDP portem 3222 (zdrojový i cílový).

AVG rozdává virtuální MAC adresy klientům deterministickým způsobem. GLBP podporuje následující operační módy pro rozdělování zátěže napříč vícero výchozích bran, které spravují stejnou IP adresu výchozí brány:

Váhové rozdělování zátěže: Kde hodnoty vah zátěže jsou rozloženy mezi účastníky GLBP. AVG na základě vah určuje frekventovanost odpovědí na ARP dotazy MAC adresami účastníků. A tím zatěžuje daný AVF směrovač.

Vyvažování zátěže na základě hostů: Každá koncová stanice generující ARP dotazy dostává vždy stejnou odpověď se stejnou MAC adresou.

Round-robin vyvažování zátěže: Odpovědi na ARP dotazy klientů se točí ve smyslu MAC adresy následujícího možného směrovače.



Obrázek 1.12: *GLBP protokol*

Směrovač R1 je AVG aktivní a rozděluje MAC adresy ostatním. Zároveň je však AVF 1 aktivní a AVF2 naslouchající. Jinými slovy, pro MAC adresu 0070.b400.0101 je aktivní výchozí bránou R1. Pro MAC adresu 0070.b400.0102 je výchozí bránou R2. Obě mají stejnou virtuální adresu 192.168.1.1. Kdyby R1 směrovač měl výpadek, tak R2 bude VGA (VG) aktivní, pro VF1 a VF2 bude také aktivním. Takže bude mít i dvě MAC adresy, ale jen určitou dobu, dokud nevyprší časovače "redirect timer" a "timeout timer". Redirect časovač určuje dobu, jak dlouho bude R2 odpovídat na ARP dotazy MAC adresou původně aktivního AVG. Výchozí hodnota je 10 minut. Timeout časovač určuje, za jak dlouho se MAC adresa původního AVG směrovače vymaže z R2. Výchozí hodnota je čtyři hodiny. [1]

2 Praktická část:

2.1 Úvod k praktické části

Za účelem ověření kompatibility zařízení společnosti Huawei a Cisco jsou v diplomové práci použity následující přepínače:

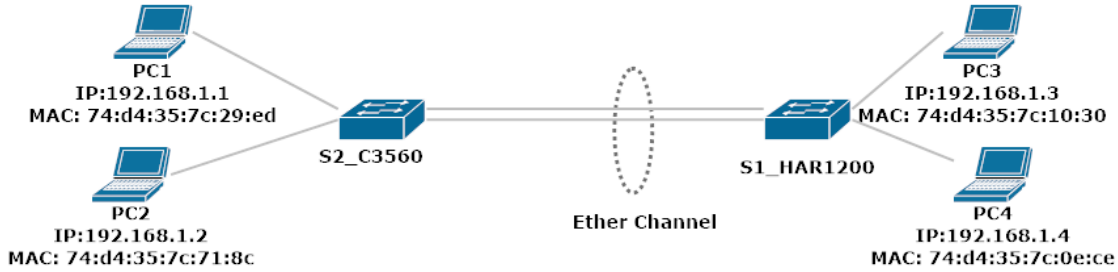
CISCO 3560 verze software 12.2(50)SE3
CISCO 2960 verze software 12.1(35)EA
Huawei Quidwai S5328C verze software 5.150
Huawei AR1200 verze software 5.120

Tato zařízení byla propojena a nakonfigurována ve třech topologiích. V každé byly zaměněny Huawei i Cisco přepínače, aby byla ověřena interoperabilita mezi různými přepínači a verzemi OS. Na vytvořených topologiích, které jsou použity v praktické části, je nastavena konvence ve formátu prvků SX_model. Jména prvků začínající písmenem označení S následovaným číslicí označují, že se jedná přepínač. Následující část model značí výrobce a typové označení produktu. Například S2_HQ5328 značí, že se jedná o přepínač číslo 2 a jedná se o výrobce Huawei model Quidwai S5328. Obdobně bude vypadat formát pro Cisco serie 3560 S1_C3560. Popis konfigurace v jednotlivých topologiích je v rámci práce stručnější, protože je řada nastavení konfigurace shodná, proto není potřeba jejich opakujícího detailního popisu. Vypíšu pouze jedenkrát kompletní konfiguraci, od které se budou ostatní odvíjet.

2.2 Redundance na linkové vrstvě.

Zapojení Etherchannel mezi dvěma přepínači různých výrobců Cisco a Huawei bylo realizováno pomocí dvou linek a vyjednáno pomocí protokolu LACP, protože LACP je otevřený protokol a je jediný, který oba výrobci podporují. Do obou přepínačů byly také zapojeny dvě klientské stanice. U značky Huawei byl použit L2 přepínač Quidway S5328, protože nabízí nejvíce možností vyvažování zátěže. U výrobce Cisco disponuje pouze model 3560 stejnými možnostmi a těmi jsou dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac. Zato Cisco řada 2960 nabízí pouze dst-mac a src-mac. Huawei přepínač AR1200 nabízí pouze jednu možnost a to sa-xor-da.

Jako měřící nástroj jsem použil Iperf pod operačním systémem LINUX Ubuntu pro ověření vyvažování zátěže. Na Etherchannel portech byla nastavena přenosová rychlost na sto megabitů za sekundu. Takže teoretická maximální propustnost svazku tvořeného dvěma rozhraními v Etherchannel tvoří dvou set megabitovou linku. Pomocí Iperf nástroje jsem ověřoval všechny druhy vyvažování zátěže. A to současně ze dvou stanic na jedné straně proti jedné, nebo dvěma stanicím na druhé straně. Taky varianta kdy jedna stanice spouští Iperf proti dvěma stanicím.



Obrázek 2.1 Zapojení Etherchannel Cisco Huawei

Provedené zapojení je realizováno podle obrázku č. 2.1. Jako hlavní rozdíl pojmenování svazku portů je u Huawei Eth-trunk a u Cisco Etherchannel. Zde popíši jednotlivé kroky v konfiguraci Etherchannel mezi přepínači.

Huawei AR1200

```
<Huawei> system-view
[Huawei]sysname S1_HAR1200
[S1_HAR1200]interface Eth-Trunk 1
[S1_HAR1200-Eth-Trunk1]port link-type access
[S1_HAR1200-Eth-Trunk1]mode lacp-static
[S1_HAR1200-Eth-Trunk1] quit
```

Řádky:

1. Příkazem se vejde do konfiguračního módu.
2. Pojmenování přepínače.
3. Vytvoření Eth-trunk 1, neboli logický port.
4. Nastavení Eth-trunk portu jako přístupový (acces).
5. Nastavení protokolu LACP.
6. Opuštění logického portu.

```
[S1_HAR1200] interface Gigabitethernet 0/0/1
[S1_HAR1200-GigabitEthernet0/0/1]eth-trunk 1
[S1_HAR1200-GigabitEthernet0/0/1]undo negotiation auto
[S1_HAR1200-GigabitEthernet0/0/1]quit
```

Další čtyři příkazy znamenají, vejití do konfiguračního rozhraní portu Gigabitethernet 0/0/1, přiřazení do Eth-trunk 1, vypnutí automatického vyjednávání ryhlosti a odejití z konfiguračního prostoru. Stejný scénář se odehrává na portu Gigabitethernet 0/0/2.

```
[S1_HAR1200]interface Ethernet 0/0/2
[S1_HAR1200-GigabitEthernet0/0/2]eth-trunk 1
[S1_HAR1200-GigabitEthernet0/0/2]undo negotiation auto
 [S1_HAR1200-GigabitEthernet0/0/1]quit
```

Tímto je nastaven LACP protokol nad dvěma rozhraními Gigabitethernet 0/0/1 a 0/0/2 na přepínači Huawei AR1200.

Následuje konfigurace Cisco C3560 přepínače:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S2_C3560
S2_C3560 (config)# interface port-channel 1
S2_C3560 (config-if)#exit
```

Řádky:

1. Vstupuje do privilegovaného módu
2. Následuje vstup do konfiguračního módu
3. Nastavení názvu přepínače na S2_C3560
4. Vytvoření logického portu Ether Channel 1
5. Odchod z konfiguračního prostoru portu.

```
S2_C3560 (config)#interface fa0/1
S2_C3560 (config-if)#channel-group 1 mode active
S2_C3560 (config-if)#exit
S2_C3560 (config)#interface fa0/2
S2_C3560 (config-if)#channel-group 1 mode active
S2_C3560 (config-if)#exit
```

Řádky:

1. Vstupuje do konfiguračního rozhraní fa0/1,
2. Nastavení, aby byl součástí Ether Channel svazku a byl nastaven jako auto (pasivní vyjednávací režim LACP).
3. Odchod z konfigurace portu
4-5. Totéž se provede na portu fa0/2.

Tímto je zajištěn Etherchannel svazek mezi dvěma zařízeními. Následuje ověření funkčnosti dané topologie. Pro měření očekávaného rozložení zátěže byl zvolen program na měření propustnosti Iperf jak bylo popsáno výše. Následující tabulka obsahuje naměřené hodnoty.

Tabulka 2.1 Měření vyvažovacích metod Cisco 3560 -> Huawei AR1200

CISCO 3560 (S2_C3560)->Huawei AR1200 (S1_HAR1200)			
metody	2pc->2pc [Mbit/s]	2pc->1pc [Mbit/s]	1pc ->2pc [Mbit/s]
dst-ip	94/94	45/49	48/48
dst-mac	52/43	46/48	49/48
src-dst-ip	94/94	94/94	47/48
src-dst-mac	30/60	94/94	48/48
src-ip	48/46	50/42	48/48
src-mac	94/94	94/94	47/48

Z tabulky 2.1 je vidět, jak se Cisco přepínač chová v jednotlivých situacích. Jednotlivé sloupce znamenají následující: 1. sloupec: metody vyvažování, 2. sloupec: propustnost dvou stanic proti dvěma, 3. sloupec: propustnost dvou stanic proti jedné a 4. sloupec měření jedné stanice proti dvěma.

V rámci Etherchannel svazku tvořeného dvěma porty rozhoduje poslední bit, kterým portem data budou téct. Pomocí bitu 0 a1 se rozhoduje, jestli datový tok poteče prvním, nebo druhým portem.

Podle prvního řádku naměřených hodnot se vše tváří jak má, ale v celém posledním sloupci tabulky, kde se měří propustnost mezi jedním počítačem proti dvěma, se hodnoty rozcházejí s teorií. V dst-ip metodě jsou cílové IP adresy různé a každý tok by měl být propouštěn jiným portem, tudíž by se mělo dosahovat hodnoty celkové propustnosti okolo 200 Mbit/s. Důvod byl zapříčiněn samotnými porty Cisco přepínače, rychlost portu mezi přepínačem a klientskou stanicí byl 100 Mbit/s, tudíž bylo nereálné dosáhnout vyšších přenosových rychlostí a zjistit jestli bude vyvažovací metoda odpovídat teorii.

V dst-mac metodě naměřených hodnot, první sloupec s hodnotou 52/43 odpovídá teorii, toky dat jdou jedním portem, proto je celková rychlost cca 100Mbit/s. Je to z důvodu MAC adres, které mají po převedení do binární podoby stejný poslední bit roven „0“. Následují hodnota (dvou stanic proti jedné) s hodnotou 46/48 vychází z toho, že cílová MAC adresa je jedna v obou tocích, proto oba toky proudí jedním portem a dosahují celkové rychlosti cca 100 Mbit/s.

U metody src-dst-ip podle prvních naměřených hodnot odpovídá tomu, že data jdou skutečně mezi dvěma porty kanálu Etherchannel. Následující pole v tabulce s hodnotou 94/94

znamená, že stanice s IP adresami 192.168.1.1 a 192.168.1.2 spouští datové toky na stanici PC4 192.168.1.4.

Z teorie je použita XOR operace na vypočtení hash hodnot ze zdrojové a cílové IP adresy, která je znázorněna níže:

Zdrojová IP adresa PC1 192.168.1.1 [001 bin]

Zdrojová IP adresa PC2 192.168.1.2 [010 bin]

Cílová IP adresa PC4 192.168.1.4 [100 bin]

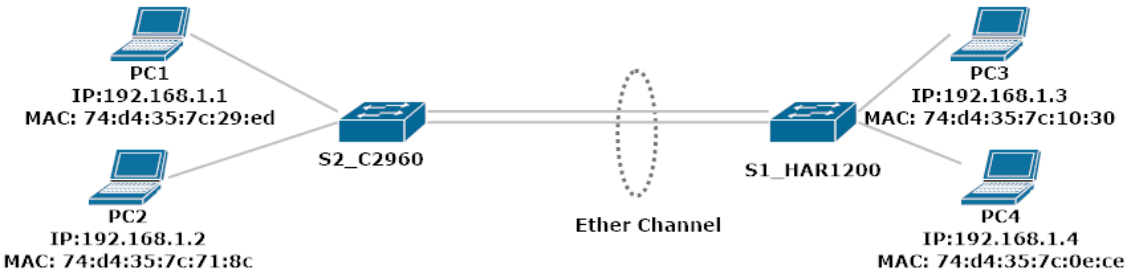
Operace XOR : (PC1) 001 xor (PC4) 100 = 101

(PC2) 010 xor (PC4) 100 = 110

Jedná se o rozložení zátěže mezi dvěma porty, takže bude podstatný pouze poslední bit vypočtené XOR operace. Datové toky mají koncové hodnoty 1 a 0. Tudíž budou téct dvěma porty. Z následující tabulky 2.2 je vidět, že jsou toky od sebe odlišeny, tudíž každý spadá do jiného portu Etherchannel svazku. Tok z PC1 na PC4 pude portem číslo dva a tok z PC2 na PC4 poteče portem číslo jedna.

Tabulka 2.2 Určení toků

		Pořadové číslo portu	port 1.	port 2.
8 portů-8 hodnot	000	1	000	
	001	2		001
	010	1	010	
	011	2		011
	100	1	100	
	101	2		101
	110	1	110	
	111	2		111



Obrázek 2.2 Zapojení Etherchannel Cisco Huawei

Zapojení podle obrázku 2.2 zobrazuje Cisco 2960 přepínač a Huawei AR1200. Cisco řady 2960 nabízí pouze dvě metody vyvažování zátěže a to dst-mac a src-mac. Následující tabulka ukazuje naměřené hodnoty.

Tabulka 2.3 Měření vyvažovacích metod Cisco 2950 ->Huawi AR1200

CISCO 2960 ->Huawei AR1200		
	2pc->2pc[Mbit/s]	2pc->1pc[Mbit/s]
dst-mac	45/48	45/48
src-mac	94/94	97/92

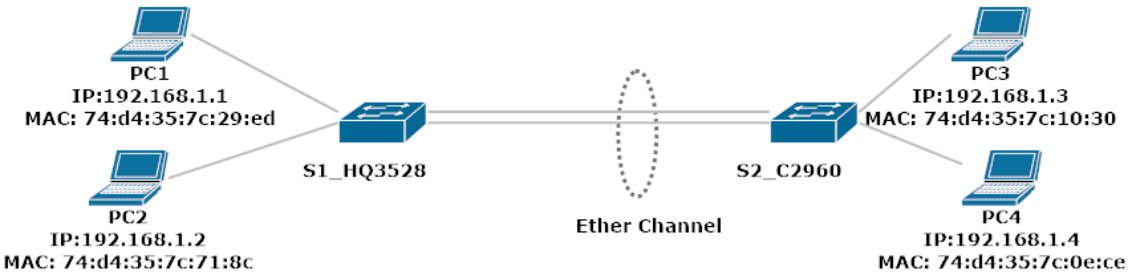
U tohoto měření docházelo dle očekávání k rozložení zátěže kromě 2pc->2pc v metodě dst-mac. Proto objasním výpočty, jak k tomu bylo docíleno:

dst-mac metoda: PC3 MAC: 74:d4:35:7c:10:30

PC4 MAC: 74:d4:35:7c:0e:ce

Převod do binární podoby 0[hex]=0000[bin]; e[hex]=1110[bin]

Jedná se o dva porty v Etherchannel, tudíž rozhodující bit bude poslední bit, který je u obou výpočtů stejný roven „0“. Dva datové toky budou na základě stejné hodnoty poslány jedním portem v Etherchannel zapojení, využitá bude tedy maximální přenosová rychlost jednoho portu, proto maximální rychlost bude rovna součtu 100Mbit/s.



Obrázek 2.3 Zapojení Etherchannel Huawei Cisco

Tabulka 2.4 Měření vyvažovacích metod Huawei Quidway S5328->Cisco3560

Huawei S5328C (S1_HQ5328-> CISCO 3560 (S2_C3560)			
	2pc->2pc [Mbit/s]	2pc->1pc [Mbit/s]	1pc ->2pc [Mbit/s]
dst-ip	94/94	46/47	94/94
dst-mac	94/94	38/56	73/23
src-dst-ip	94/94	53/40	94/94
src-dst-mac	37/57	48/48	40/50
src-ip	94/94	50/40	94/94
src-mac	60/37	50/43	27/64

U tohoto měření již třetí sloupec „1pc ->2pc“ obsahuje relevantní data. Na druhou stranu hodnoty obsahující druhý sloupec „2pc->1pc“ dosahují maximálně součtu do 100Mbit/s protože linka mezi Cisco přepínačem a klientskou stanicí je pouze 100Mbit/s. Nelze zde použít teorii, která je opřená o Cisco přepínače. Tudíž nemohu nastínit vyvažovací algoritmy.

Tabulka 1.6:

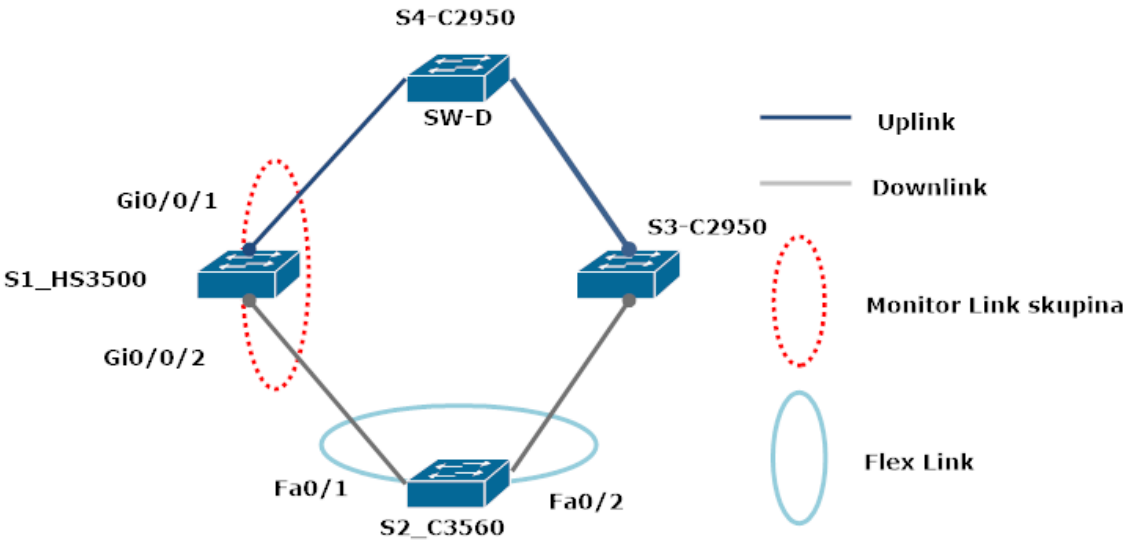
2.2.1 **Monitor Link a Flex Link**

V následujícím zapojení jsem kombinoval dvě proprietární techniky Monitor Link od Huavei spolu s Flex Link od Cisco společností. Monitor Link funkcionalita spočívá v hlídání definovaného portu označeného jako „uplink port“ a vypínání, nebo zapínání jednoho, nebo několika portů označených jako „downlink port“. Jakmile na uplink portu dojde k výpadku, tak

Monitor link vypíná downlink porty. Tahle funkcionalita je v porovnání se STP protokolem rychlejší, pracuje v řádech milisekund.

Flex Link je technika od společnosti Cisco podobná Smart link u Huawei. Princip spočívá na hlídání aktivního portu, který přeposílá data. A nahození záložního portu v případě kdyby aktivní port selhal.

V zapojení jsem simuloval výpadek portu Gi0/0/1 na Huawei přepínači S1_HQ3528 a sledoval, jak Monitor Link vypne „down link“ port Gi0/0/2 , poté co přepínač Cisco S2_C3560 zjistí, že port fa0/1 má výpadek, tak pomocí Flex Link přepne z již neaktivní linky fa0/1 na záložní fa0/2 a data potečou skrze nový port fa0/2.



Obrázek 2.4 Monitor Link a Flex Link

Následující příkazy slouží k vytvoření Monitor Link skupiny 1, nastavení Gigabitethernet 0/0/1 jako uplink a Gigabitethernet 0/0/2 jako downlink port.

```
[S1_HQ5328] monitor-link group 1
[S1_HQ5328-mtlk-group2] port gigabitethernet 0/0/1 uplink
[S1_HQ5328-mtlk-group2] port gigabitethernet 0/0/2 downlink
```

Pomocí následujícího příkazu si ověříme správné nastavení:

```
display monitor-link protocol-parameter group 1
```

```
[Quidway]display monitor-link protocol-parameter group 1
MONITOR-LINK Group 1:
*********************************
 *RecoverTime:       3 sec.
 *TimeCounter:       2 sec.
 *Uplink Info:
  IfIndex:           6(GigabitEthernet0/0/1)
  PortType:          2(MTLK_PORT SWITCH)
  LinkStatus:        0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Downlink 1 Info
  IfIndex:           7(GigabitEthernet0/0/2)
  LinkStatus:        0(down)
  IsShutdown:        1(shutdown)
```

Obrázek 2.5 Výpis monitor-link nastaverní

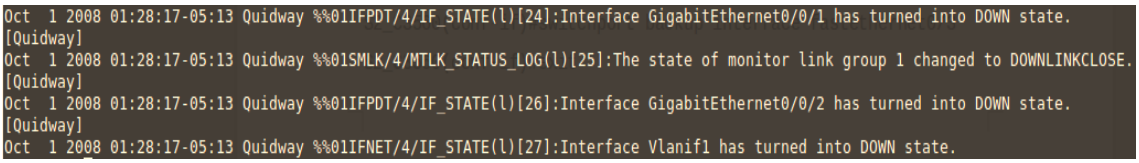
Ve výpisu je vidět, že ulink port je GigabitEthernet 0/0/1 a Downlink je Gigabitethernet 0/0/2.

Konfigurace Flex Link na portu FastEthernet 0/2 který pracuje jako primární a FastEthernet 0/3 jako záložní: je následující:

```
Switch# configure terminal
S2_C3560(conf)#interface fastethernet0/2
S2_C3560(conf-if)#switchport backup interface fastethernet0/3
S2_C3560(conf-if)#exit
```

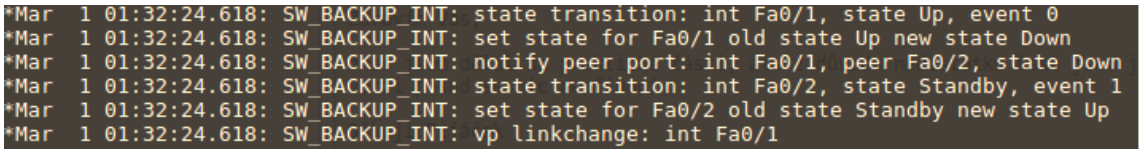
Pomocí příkazu "switchport backup interface fastethernet 0/3" se nastavuje port fa0/3 jako záložní port pro fa0/2. Má status "UP" ale nepropouští žádné data, tím zabraňuje vzniku smyčky.

Následující obrázek vypisuje ladění "debug" při výpadku nadefinovaného Uplink portu na přepínači Huawei S1_HQS3528, kde je i popsáno, že downlink port se vypíná pomocí Monitor Link.



Obrázek 2.6 Debug Monitor Link

V následujícím obrázku je detailní výpis dění, při kterém probíhá k přepnutí na zálohu u přepínače Cisco, kterou zapříčinil Monitor Link na přepínači Huawei.



Obrázek 2.7 Debug Flex Links

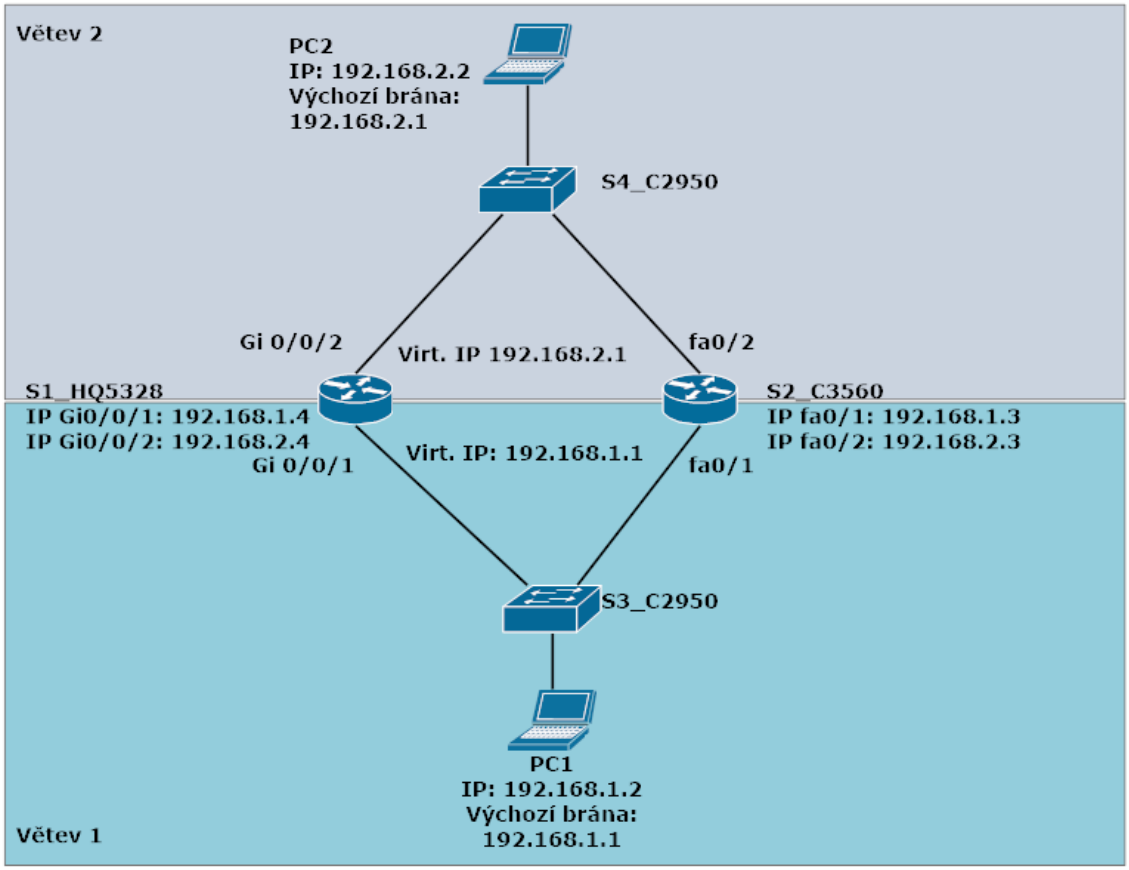
První řádek informuje, že rozhraní Fa 0/1 je v pořádku. Následně odpojím kabel od portu Fa0/1. Druhý řádek píše, že port Fa0/1 má výpadek, následně ve třetím řádku je upozorněn port Fa0/2 o tomhle dění. Na čtvrtém řádku je zjištěn stav rozhraní Fa0/2 a na čtvrtém řádku je přepnut ze záložního Standby na aktivní Up.

Zapojení pracovalo dle očekávání, po opětovném nahození portu a Huawei přepínači S1_HQ3528 došlo k nahození down link portu Gi0/0/2 a po chvíli i původně aktivního portu fa0/1 na přepínači S1_HQ5328.

2.3 Redundance na síťové vrstvě

V topologii zapojení redundantní výchozí brány byl zvolen protokol VRRP na obou směrovačích dle obrázku č. 2.5. Je to jediný společný protokol, který podporují oba výrobci. Zapojení má vlastnost zálohy výchozí brány pro větev jedna a dvě, neboli pro klientské stanice PC1 a PC2. U tohoto protokolu na rozdíl od GLBP může být ve VRRP skupině pouze jedna brána aktivní a přeposílat data a druhá jako záložní bez účasti přeposílání.

Zapojení se skládá ze dvou sítí, které se nacházejí ve dvou větvích. Síť 192.168.2.0/24 se nachází ve větvi 2 a síť 192.168.1.0/24 se nachází ve větvi 1. Oba směrovače jsou členy dvou VRRP skupin, které jsou rozděleny taktéž do dvou větví VRRP1-větev1, VRRP2-větev2. Směrovače jsou nakonfigurovány pomocí priorit tak, aby každý z nich byl Master směrovačem v jedné větvi (v jedné síti). Tím se zajistí, že se každý směrovač bude aktivně podílet na přeposílání dat. Směrovač Huawei S1_HQ5328 bude Master směrovačem pro VRRP skupinu číslo 1 ve větvi 1. Směrovač Cisco S2_C3560 bude Master směrovačem VRRP 2 ve větvi 2. Tím se docílí statického rozprostření zátěže. Data z PC1 půjdou přes S1_HS350 do sítě 192.168.2.0/24 a data z PC2 půjdou přes S2_C3560 do sítě 192.168.1.0/24.



Obrázek 2.8 VRRP zapojení

V případě tohoto zapojení je důležité zapnout dodatečnou funkci, která monitoruje rozhraní na lokálním směrovači. Na základě toho přenastaví hodnoty priorit ve VRRP skupině, jinak by mohlo dojít k výpadkům dostupnosti. Funkce se nazývá u obou výrobců stejně „track“ a může být nastavena, aby hlídala dostupnost IP adresy, nebo portu.

Pokud by „track“ nebyl nastaven na obou směrovačích, tak v případě výpadku portu fa0/1 na směrovači S2_C3560 dojde k přerušení spojení ve směru z PC2 na PC1. Je to zapříčiněno tím,

že se stav ve VRRP 1 skupině nacházející se ve větvi 1 nezmění, protože S1_HQ5328 je Master pro tuto větev a výpadek Slave směrovače pro něj nic neznamenají. VRRP 2 skupina se také nepřepne z Master směrovače který zastává S2_C3560 na Slave, protože nemá nic společného se skupinou VRRP1. Takže data z PC2 směrující na PC1budou zahazována směrovačem S2_C3560, který zastává Master funkci ve větvi 2.

Následuje popis konfigurace VRRP protokolu spolu s „track“ funkcí:

Ve výchozím nastavení mají oba výrobci stejnou prioritu ve VRRP protokolu s hodnotou 100. Tudíž by se stal Master směrovačem, který bude přeposílat data v obou větvích Huawei S1_HQ5328 díky vyšším IP adresám v obou sítích. V tomhle zapojení budou nastaveny

priority manuálně, zajistí se tím určité opatření v situacích, kdyby se do topologie přidávaly další redundantní směrovače.

Následující dva řádky znamenají zapnutí dvou již zmíněných sledování, track 1 a track 2, kde každé sleduje jeden port.

```
S2_C3560(conf)#track 1 interface fastethernet0/1 line-protocol
S2_C3560(conf)#track 2 interface fastethernet0/2 line-protocol
```

V následujících řádcích se nastavuje po IP adrese na rozhraní další IP adresa, která bude virtuální v instanci VRRP 2. Stejné číslo instance musí mít nastaven i druhý směrovač na portu ve stejné větvi, jinak by zapojení bylo nestabilní. Předposlední příkaz znamená, že k VRRP 2 instanci připojuji sledování „track 1“, které jsem si připravil v předchozích řádcích. Které sleduje port fa0/1 ve větvi 1.

```
S2_C3560(conf)#interface fastethernet0/2
S2_C3560(conf-if)#ip address 192.168.2.3 255.255.255.0
S2_C3560(conf-if)#vrrp 2 ip 192.168.2.1
S2_C3560(conf-if)#vrrp 2 priority 150
S2_C3560(conf-if)#vrrp 2 track 1 decrement 20
```

Když bude mít fa0/1 výpadek, tak se poníží priority hodnota díky funkci track 1 na VRRP 2 a směrovač S1_HQ5328 se díky vyšší prioritě stává Master směrovačem ve větvi 2. Tímto se díky výpadku jednoho portu ovlivňuje chování dalšího portu v jiné VRRP skupině. Je tak docíleno zálohovaného redundantního zapojení výchozích bran s možností rozdělení zátěže.

Následující konfigurace je obdobná předchozí, nebudu k ní uvádět komentáře.

```
S2_C3560(conf)#interface fastethernet0/1
S2_C3560(conf-if)#ip address 192.168.1.3 255.255.255.0
S2_C3560(conf-if)#vrrp 1 ip 192.168.1.1
S2_C3560(conf-if)#vrrp 1 priority 140
```

```
S2_C3560(conf-if)#vrrp 1 track 2 decrement 20
S2_C3560(conf-if)#exit
```

Na směrovači Huawei vypadá konfigurace podobně, jen jsou zredukovány dva řádky na jeden v případě zapnutí sledování portu „track“.

```
[S1_HQ5328]interface GigabitEthernet 0/0/1
[S1_HQ5328-GigabitEthernet0/0/1]ip address 192.168.1.4
255.255.255.0
[S1_HQ5328-GigabitEthernet0/0/1]vrrp vrid 1 priority 150
[S1_HQ5328 GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip
192.168.1.1
[S1_HQ5328-GigabitEthernet0/0/1]quit
[S1_HQ5328-GigabitEthernet0/0/1]vrrp vrid 1 track
Gigabitethernet 0/0/2 reduced 20
[S1_HQ5328]interface GigabitEthernet 0/0/2
[S1_HQ5328-GigabitEthernet0/0/2] ip address 192.168.2.4
255.255.255.0
[S1_HQ5328-GigabitEthernet0/0/1]vrrp vrid 2 priority 140
[S1_HQ5328-GigabitEthernet0/0/2]vrrp vrid 2 virtual-ip
192.168.2.1
[S1_HQ5328-GigabitEthernet0/0/2]vrrp vrid 2 track
Gigabitethernet 0/0/1 reduced 20
```

V zapojení byla ověřena teorie s laboratorními podmínkami. Po výpadku portu fa0/1 směrovače Cisco došlo k ponížení priority ve skupině VRRP2 a směrovač Huawei si převzal funkci Master směrovače ve VRRP2 skupině díky vyšší prioritě. Po opětovném zapojení portu fa0/1 nedochází ke zpětnému přehození, jestli není nastavena volba „preemption“ která umožňuje, aby se směrovač s vyšší prioritou opět stal Master směrovačem ve VRRP skupině. Zapojení bylo bez potíží sestaveno a ověřeno.

Závěr

Cílem diplomové práce bylo navrhnout a popsat možnosti využití redundantního zapojení mezi přepínači a směrovači společnosti Cisco a Huawei. Následně bylo provedeno zapojení v laboratorních podmínkách pro ověření teoretických poznatků. Pro jednotlivé redundantní zapojení byla navržena vhodná topologie, která umožňovala nasazení protokolů.

Z praktických zapojení bylo dokázáno, že pomocí technologie Etherchannel se přenosová rychlost zvětší jen za určitých podmínek. K docílení maximálního potenciálu technologie Etherchannel musí být zajištěn různorodý druh provozu. Díky tomu můžou vyvažovací metody na jeho různorodých vlastnostech využívat více portů, než kdyby byl druh provozu stejnorodý. Pokud jsou na koncích Etherchannel přepínačů směrovače, tak lze použít pouze vyvažovacích metod na síťové, nebo transportní vrstvě. Co se nedá upřít Etherchannel technologii je levný a efektivní způsob postavení topologie s redundantními spoji zajišťující určitý druh vysoké dostupnosti. V linkové vrstvě Etherchannel snižuje počet smyček, které by jinak musel blokovat STP protokol, nebo jiné proprietární řešení. V síťové vrstvě lze pomocí Etherchannel snížit počet použitých IP adres a tím spojené směrovaní. V práci také byly nasazeny proprietární technologie, které zajišťují redundantní spojení a zároveň nabízí kratší časy konvergence v porovnaní se STP protokolem.

Diplomovou práci bych doporučil ve školství, stejně tak i v komerční sféře. Poskytovatelé internetového připojení se rádi drží jedné značky, jednoho výrobce. Je to logické, neboť tím získávají možnost využití proprietárních funkcí napříč celou sítí a taky nemusí nakupovat více druhů zařízení. Může ale nastat situace, kdy technik, nebo student bude muset řešit redundantní spojení i mezi prvky různých výrobců. Pomocí diplomové práce získá přehled, jaké možnosti se nabízejí i s konkrétními případy. Na diplomovou práci se dá navázat pokročilejšími technikami, jako jsou Multi-Chassis Link Aggregation Group (M-LAG) jejichž implementace spočívá v pokročilejších technikách redundance mezi více prvky.

Použitá literatura

[1] FROOM, Richard a Erum FRAHIM. Implementing Cisco IP switched networks (SWITCH) foundation learning guide. Indianapoils, IN: Cisco Press, 2015. ISBN 978-1-58720-664-1.

[2] Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(53)SE2 - Configuring Etherchannels [Cisco Catalyst 3750-X Series Switches] - Cisco. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_53_se/configuration/guide/3750xscg/swethchl.html

[3] Cisco network technology - Cisco Network Technology. Cisco Network Technology - Cisco network technology [online]. Dostupné z: https://cisco3750x.weebly.com/cisco-network-technology/Etherchannelload-balance-hash-algorithm

[4] Distributing Traffic in Etherchannel - 37841 - The Cisco Learning Network. [online]. Copyright © 2007 [cit. 29.04.2018]. Dostupné z: https://learningnetwork.cisco.com/message/199965#199965

[5] Cisco - Global Home Page [online]. Copyright © [cit. 29.04.2018]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.pdf

[6] Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(53)SE1 - Configuring STP [Cisco Catalyst 2960 Series Switches] - Cisco. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swstp.html

[7] HUAWEI Smart Link & Monitor Link Technology White Paper On Line View. [online]. Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved. [cit. 29.04.2018]. Dostupné z: http://e.huawei.com/en/marketing-material/onlineview?materialid=%7B39fc53db-b088-4aaa-a72d-eca9535b09f8%7D

[8] Configuring Flex Links - Cisco. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/swflink.html

Seznam příloh

Součástí BP/DP je CD/DVD.

Adresářová struktura přiloženého CD/DVD:

Příloha A: *Naměřené hodnoty*

Tabulka A.1: *Větší tabulka naměřených hodnot*

Tabulka A.2: *Jiná tabulka*

Příloha B: *Velká tabulka na celou stránku*

text							